Departamento de Derecho Público y
Filosofía Jurídica
Programa de Doctorado en Derecho,
Gobierno y Políticas Públicas

Tesis Doctoral

La gestión de datos personales y el delegado de protección de datos en la sanidad pública. Con atención especial a la Comunidad de Madrid.

DIRECTORA
Blanca Rodríguez-Chaves Mimbrero

DOCTORANDO
Juan José Bestard Perelló

Fecha de la última finalización, fecha de impresión o PDF del documento: 30 de mayo de 2021

Tesis Doctoral

La gestión de datos personales y el delegado de protección de datos en la sanidad pública. Con atención especial a la Comunidad de Madrid

INDICE POR TÍTULOS, CAPÍTULOS Y EPÍGRAFES pg

Índice de Tablas

Índice de abreviaturas y siglas

AAPP	Administraciones Públicas
ADFUE	Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa
AEC	Asociación española de calidad
AEMPS	Agencia Española del Medicamento y Productos Sanitarios
AEPD	Agencia Española de Protección de Datos
BCR	Binding Corporate Rules (Normas corporativas Vinculantes)
BOE	Boletín Oficial del Estado
C.c.	Código Civil
CE	Constitución Española
CEPD	Comité Europeo de Protección de Datos
CNI	Centro nacional de inteligencia
CIE-10	Clasificación internacional de enfermedades, 10.ª edición
CIP-AUT	Código de identificación personal asignado por la administración sanitaria emisora de la tarjeta
CIPSNS	Código de Identificación personal del Sistema Nacional de Salud
CIP-SNS	Código de Identificación personal del Sistema Nacional de Salud
CITE	Código administración sanitaria emisora de la tarjeta
CMBD	Conjunto Mínimo Básico de Datos
COVID	Coronavirus desease
CPS	Certificado provisional sustitutorio
CS	Centro de Salud
CSM	Consejería de Sanidad de Madrid
DIN	Deutsches Institut für Normung Instituto Alemán de Normalización
DNI	Documento Nacional de Identidad
DPO	Data Protection Officer delegado de protección de datos
DUDH	Declaración Universal de Derechos Humanos
ECDC	Centro europeo para la prevención y el control de las enfermedades
EE.UU	Estados Unidos de América
EIPD	Evaluación del Impacto en la Protección de Datos
ENAC	Entidad Nacional de Acreditación
ENI	Esquema Nacional de Interoperabilidad
EPIETEN	Programa Europeo de Formación en Epidemiología de Intervención
EUPHEMEN	Programa Europeo de Formación en Microbiología para la Salud Pública
FD	Fundamento de derecho
FDS	Factores determinantes de la salud
FJ	Fundamento jurídico
FFJJ	Fundamentos jurídicos
FIB	Fundación de investigación Biomédica
GDRs	Diagnosis Related Groups Grupos de pacientes Relacionados por el Diagnóstico
GPEIPD	Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos
HC	historia clínica
HIA	Health Impact Assesment
IdiPAz	Instituto de Investigación sanitaria del Hospital Universitario La Paz

IDIS	Instituto para el desarrollo e intergacion de la sanidad
Ig	Inmunoglobulina
INC	Incorporation (corporación con personalidad jurídica)
IIS	Institutos de Investigación sanitaria
ISFAS	Instituto Social de las Fuerzas Armadas
ISO	International Organization for Standardization
LPAC	Ley del Procedimieto Administartivo Común de las Administraciones Públicas
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPDGDD	Ley de protección de datos personales y garantía de los derechos digitales
MUFACE	Mutualidad General de Funcionarios Civiles del Estado
MUGEJU	Mutualidad General Judicial
NIE	Número de identidad de extranjeros
OMS	Organización Mundial de la Salud
ONS	Oficina nacional de seguridad
ONU	Organización de las Naciones Unidas
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
RAE	Real Academia Española
RGPD	Reglamento General de Protección de Datos
SARS-Cov-2	Severe acute respiratory syndrome coronavirus 2
S.L.	Sociedad Limitada o Sociedad de Responsabilidad Limitada
SERMAS	Servicio Madrileño de Salud
SIP-CIBELES	Sistema de Información Poblacional de la Comunidad de Madrid
SNS	Sistema Nacional de Salud
SSTC	Sentencias del Tribunal Constitucional
STC	Sentencia del Tribunal Constitucional
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo
SUMA	Servicio de urgencias médicas de Madrid
TCFA	Tribunal Constitucional Alemán
TESSY	The european survillance system
TFUE	Tratado de Funcionamiento de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tratado de la Unión Europea
UE	Unión Europea
UNE	Asociación Española de Normalización
UNE-EN	Una norma española-European Norm
WHO	World Health Organization
WHO-FIC	Red de la Familia de Clasificaciones Internacionales de la OMS

RESUMEN

La Tesis parte de la hipótesis de la existencia de disfuncionalidades en la aplicación del Reglamento General de Protección de Datos (Reglamento (UE) 2016/679, RGPD) en el ámbito de la sanidad. Dichas disfuncionalidades se detectan tanto en lo que corresponde a la aplicación del Reglamento General de Protección de Datos en el ámbito procedimental, con la aplicación de los principios, derechos, y la propia base jurídica que legitima la gestión de los datos personales, entre otros, como la aplicación de dicho Reglamento (UE) 2016/679 en el ámbito organizativo, sobre todo en lo referido a la implantación de la figura del delegado de protección de datos, como garantía de aplicación del propio Reglamento General de Protección de Datos. Dichas disfuncionalidades se han puesto de relieve durante el proceso de gestión de la alarma sanitaria causada por la pandemia COVID-19 y su conjunción con el respeto al derecho fundamental a la protección de datos de carácter personal. Durante el trascurso de la Tesis se analizan especialmente dichas disfuncionalidades en el ámbito de la sanidad pública Comunidad de Madrid, siendo dicho análisis extensible al sector sanitario público español y se aportan soluciones jurídicas para que se haga efectiva la aplicación del RGPD.

La tesis se inicia con el estudio del dato en profundidad, lo cual obliga a entrar en la definición de concepto de dato personal o datos sobre las personas, en definitiva, el elemento fáctico del derecho fundamental que se protege. En este sentido, dato es aquella realidad o hecho captado por el ser humano que una vez se junta con otra realidad es capaz de aportar información o transmitir información sobre esta realidad. Dato e información no son sinónimos.

El dato personal o de una persona es el que puede aportar información relativa a un individuo identificado o identificable, el resto es dato anónimo. Desde la STS 6188/1996 se ha dejado de utilizar la expresión “datos de carácter personal” en su lugar se utiliza la expresión “dato personal”. El Reglamento (UE) 2016/679 define los datos personales como toda información sobre una persona física identificada o identificable («el interesado») y que, en opinión de la Tesis, cae en el error de confundir dato e información. No es inhabitual que se confunda dato con dato informático, por lo cual la Tesis ha profundizado en el tipo de dato sujeto al RGPD deduciendo que el Reglamento (UE) 2016/679 hace referencia a todo tipo de soporte que pueda contener un dato y a todo dipo de dato que permita la identificación de una persona.

El RGPD y la Ley Orgánica 3/2018 hacen mención a muchos tipos y subtipos de datos, como mínimo se han detectado en el anexo C un listado de treinta expresiones que califican al dato y en consecuencia lo diferencian. Sin embargo, el RDGP define básicamente dos grandes tipos de datos, los datos afectados por el RDPG y los datos que están fuera del ámbito del RGPD. Dentro del grupo de datos que están bajo el paraguas del RGPD están, por una parte, aquellos datos calificados como categorías especiales,

cuyo tratamiento está prohibido salvo excepciones, y, por otra parte, el resto de datos personales no incluidos en estas categorías, cuyo tratamiento requiere cumplir con las bases jurídicas de licitud. Las categorías especiales de datos son diez, esto es, los de origen étnico o racial, opiniones políticas, convicciones religiosas, convicciones filosóficas y de afiliación sindical, así como, datos genéticos, datos biométricos, datos de la salud, datos relativos a la vida sexual o las orientaciones sexuales de una persona física. La Tesis se detiene en el dato de origen étnico o racial, pues si bien esta incluido como categoría especial el considerando cincuenta y uno manifiesta que la Unión Europea no acepta la existencia de raza humanas separadas.

La protección de los datos personales corresponde a un derecho fundamental, tanto en España como derecho fundamental autónomo independiente al derecho a la intimidad, en base al artículo 18 de la Constitución y a la STC 292/2000, como en el régimen jurídico de la Unión Europea en base al artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Al referirnos a un derecho fundamental y al constatar durante el proceso de investigación de la Tesis que algunos temas plantean situaciones en las cuales los derechos fundamentales entran en conflicto entre sí o con bienes jurídicos protegidos, ha conducido que la Tesis haya estudiado la doctrina constitucional y del Tribunal Constitucional en relación a esta materia. En el año 2020 la OMS declaró la alarma sanitaria de la pandemia COVID-19, esta situación provocó que el Gobierno activara el protocolo para la instauración del Estado de Alarma (Ley Orgánica 4/1981, de 1 de junio), mediante el Real Decreto 463/2020, de 14 de marzo. La gestión de la pandemia ha conllevado la puesta en marcha de determinadas medidas que implican tanto la limitación del contacto entre personas como en la utilización de sus datos personales y datos personales relativos a la salud para el control de los contagios y de la transmisión de la infección, entrando en conflicto varios derechos fundamentales, entre ellos el derecho de la protección de datos y el de libre movilidad y circulación con el bien jurídico de la protección de la salud, manifestando, a su vez, una clara carencia de base regulatoria en España.

Una vez abordado el concepto jurídico de dato y de derecho fundamental, se entra de lleno en las cuestiones esenciales de la regulación del derecho fundamental de la protección de datos personales que son sin duda los principios de la protección y del tratamiento de datos de la normativa y los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de datos personales.

Toda la actividad de tratamiento de datos consiste en una sucesión de actuaciones regladas que deben desempeñar los responsables y/o los encargados del tratamiento de tales datos, es decir, en un procedimiento. Con ello, se intenta asegurar que la toma de decisiones sobre el tratamiento se ajustará a la Ley y, además, que se encaminará hacia una situación de equilibrio en los intereses del responsable y/o encargado del tratamiento y el titular de los datos, lo que, nuevamente, nos conduce a una idea de justicia material. De esta forma, bien podemos afirmar que la adhesión a esa sucesión de actuaciones determinará que el tratamiento sea legal y, también, que sea justo.

Si queremos trazar un esquema del *iter* procedimental del tratamiento de datos, sería el siguiente: en primer lugar, se deben determinar los medios del tratamiento y se debe realizar una evaluación previa de riesgos; en segundo lugar, hay que concretar el fundamento de licitud del tratamiento, es decir determinar si existe base jurídica para dicho tratamiento, bajo alguno de los supuestos de los artículos 6 ó 9 del Reglamento (UE) 2016/679; seguidamente y en tercer lugar, hay que recoger los datos con unos fines determinados, explícitos y legítimos; en cuarto lugar, se deben registrar y almacenar los datos, para lo cual se crearán los correspondientes ficheros y se llevará a cabo un registro de actividad; después, en quinto lugar, se llevará a cabo el tratamiento en sí de los datos, entendiendo por tratamiento cualquier operación realizada sobre los datos o conjunto de datos, en aplicación de los de los principios y derechos, y, en última instancia, se deberá proceder a la destrucción de los datos, ya sea mediante borrado, ya mediante bloqueo.

Esta revisión de las cuestiones procedimentales esenciales se complementa necesariamente con un estudio de las instituciones de control, regulación, tratamiento, cooperación y autorregulación del reglamento general de protección de datos. En esta descripción incluyen todos los institutos jurídicos de control y autoridad, Autoridad de control, que regulan la aplicación del Reglamento, trayendo a colación dos herramientas importantes del órgano de control, estas son, el acto de ejecución y la decisión de adecuación. Paso seguido se aborda la descripción y funciones de los tres elementos sobre los que se sustenta el principio de proactividad y el principio de autorregulación, estos son el responsable del tratamiento, el encargado del tratamiento y el delegado de protección de datos. De entre esas funciones destaca el registro de actividades, la protección del diseño y la notificación de la violación de la seguridad de los datos, así como los proyectos de Evaluación del Impacto en la Protección de Datos personales de cualquier tratamiento y en especial el de las categorías especiales y, en base a la Tesis, la necesidad de incluir los, conocidos, Mapas de Riesgo.

En este orden de cosas, la Tesis centra la cuestión y describe los aspectos nucleares del Reglamento, estos son, el objeto (la protección del dato personal), la organización (la estructura institucional), el funcionamiento (garantías y control) y el régimen jurídico (derechos y reclamaciones), con apoyo de fundamentación jurídica y doctrinal sobre la naturaleza de la norma que la Tesis estudia. Seguidamente a este enfoque inicial, se entra específicamente sobre la consideración del dato relativo a la salud, especialmente protegido, tanto en su interpretación estricta como en la versión amplia y extensa a la que hace referencia el Reglamento.

El análisis del "dato" se realiza con base en dos pilares. El primero, los tratamientos a los que se puede someter al dato personal y los elementos que los componen, es decir, elementos básicos, complementarios y adicionales, tanto cuando se refiere al dato personal como al dado personal en el sector sanitario. El segundo, en lo referente a la salud se descrinen sus tres fuentes fundamentales, estas son, la historia clínica, la receta y la tarjeta sanitaria. La Tesis resalta la importancia del control de estos datos pues están sometidos a una cierta vulnerabilidad a través del dato denominado "código de

identificación personal" que conecta la historia clínica con la tarjeta sanitaria y con la recta. Es decir, el tratamiento del dato relativo a la salud se realiza conjugando dos cuestiones tratadas en la Tesis, por una parte, la clasificación de los tres elementos del tratamiento de datos y, por otra parte, los tres soportes fundamentales de los datos personales en el sector sanitario, que en la Tesis también se entienden como sus fuentes datos.

El estudio del dato personal en el sector sanitario también se ha realizado en su vertiente organizativa, trasladando a la perspectiva sanitaria tanto la Autoridad de control como el responsable y encargado del tratamiento y finalmente el delegado de protección de datos utilizando como ejemplo, en este último caso, la aplicación del Reglamento General de Datos que ha llevado a cabo la Consejería de Sanidad de la Comunidad de Madrid y concretamente la opción de designación de un solo y único delegado de protección de datos para todos los centros sanitarios públicos.

La figura del delegado de protección de datos y, más concretamente en el sector de la sanidad pública, se aborda integralmente y de forma completa, una vez vistos y analizados todos los aspectos que pueden influir en él. Se detalla la designación y los casos obligados de designación expuestos tanto en el Reglamento (UE) 2016/679 como en la Ley Orgánica 3/2018. La Ley Orgánica 3/2018 en su artículo 34.1.L), determina el deber de designación de delegado de protección de datos en "Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes". Obligación que además queda reflejada el régimen de disciplinario del RGPD y en especial en el artículo 73 de la Ley Orgánica 3/2018 cuando califica de infracción grave "el incumplimiento de designación obligada del delegado de protección de datos".

La figura del delegado de protección de datos, en primer lugar, debe abordarse desde su nexo o conexión con el Reglamento, es decir, desde la figura del responsable del tratamiento de datos, pues una vez identificado este o, en su caso, el encargado contratado por el responsable, y en base a la naturaleza de la organización y a la de los datos necesarios, se conoce en donde existe el deber de asignar y designar un delegado de protección de datos. En segundo lugar, debe abordarse desde su relación con el objeto del Reglamento General de Protección de Datos y de la Ley Orgánica 3/2018, es decir, la protección de los datos personales y en este caso, la protección de los datos personales en el sector sanitario que incluye la protección de los principios que proclama el RGPD y los derechos a los que puede acogerse la persona para hacer efectivo su derecho fundamental de protección de su intimidad y privacidad a través del control de sus datos.

El estudio de la figura del delegado de protección de datos ha llevado a la Tesis a analizar la aplicación del RGPD en lo que se refiere al Delegado de Protección de Datos (también, DPO) en la sanidad pública de la Comunidad de Madrid. La Consejería de Sanidad opto en el año 2018 por la creación de un Comité Delegado de Protección de Datos que sustituye al DPO que debe tener cada centro sanitario en base a la Ley Orgánica 3/2018. La Tesis se detiene en la resolución PS/00417/2019 de 9 de junio de 2020 de la AEPD mediante la cual sanciona a la empresa GLOVOAPP23, S.L. por infracción graves por no

disponer de delegado de protección de datos a pesar de que la empresa alega disponer de un Comité de Protección de datos.

La Tesis no podría ni debería cerrarse sin una propuesta constructiva que tuviera en cuenta la complejidad de la aplicación del RGPD y la complejidad intrínseca del sector sanitario. Así pues, cabe decir que del conjunto del análisis de la Tesis se deduce un modelo pragmático al que puede acogerse cualquier administración nacional y/o regional para una correcta aplicación de la figura del delegado de protección sanitaria en el sector público de la sanidad.

Este modelo de aplicación alude a los principios básicos de la organización, que son: análisis-detección, priorización, diseño, control y participación de las partes implicadas. Finalmente, se hace referencia a uno de los putos importantes del principio de proactividad y autocontrol, la creación de códigos de conducta. Se propone el diseño de un manual de aplicación del RGPD en el sector de aplicación como el método consensuado y base estratégica, como precursor de la creación del código de conducta del sector de la salud.

Finalmente, unos comentarios en relación a unos aspectos criticados por la Tesis. Durante la elaboración de la Tesis se realizan hallazgos y conclusiones parciales sobre cuestiones concretas que afectan a algunos de los temas tratados. En este orden de cosas, al estudiar el dato destaca una “nota crítica” (página 33) en relación a que RGPD confunde el concepto de dato e información, no siendo estos sinónimos.

Se discute en una “nota crítica” (página 239) que el RGPD mencione que la adhesión a un Código de Conducta es sinónimo de demostrar la existencia de garantías suficientes, cuando esta adhesión lo único que demuestra es la intención de quien se adhiere, pero no su cumplimiento.

En el momento de que a Tesis entra en la cuestión de la respuesta del sistema sanitario a la demanda asistencial creada por la pandemia, se ha puesto de manifiesto que no se dispone (a 30/04/2021) todavía de la Red de Vigilancia de Salud Pública que obliga el artículo 13 de la Ley 33/2011 y se sigue funcionando con la Red nacional de vigilancia epidemiológica creada en 1995 (página 167). Además, en la página 167 a través de una “nota crítica” se deduce que en España una vez pasados los primeros meses en la gestión de la pandemia, se tenía que haber aprobado una Ley Orgánica que regulará la adopción de las medidas necesarias referidas al tratamiento de datos personales que adoptará el Gobierno y la Administración, medidas que tendrán que respetar las garantías mínimas contenidas en el RGPD.

La Tesis en una “nota crítica” (página 318) pone de manifiesto su desacuerdo en que la AEPD entiende que el profesional de la salud no estará obligado el solicitar consentimiento a los pacientes para la recogida y utilización de datos personales y de salud.

En cuanto a innovaciones a destacar. La Tesis estudia el tratamiento de datos reflejados en la normativa referida entendiendo que incluyen muchas acciones, operación o

acciones y que una vez ordenadas surge una nueva clasificación organizada en base a sus componentes, estos son, los elementos básicos del tratamiento, los complementarios y los adicionales. Esta clasificación se aplica al dato relativo a la salud en cada una de sus tres principales fuentes, estas son, la historia clínica, la receta y la tarjeta sanitaria. Por otra parte, se estudia la licitud del tratamiento de datos tanto en su vertiente general como en la sanitaria y que, arrancando de la teoría general sobre la legitimación, que engloba a la ordinaria y el extraordinario, se describen los tipos de legitimación que aparecen el RGPD, estas son, la legitimación subjetiva y la legitimación objetiva. Al tratar el secreto profesional como una de las bases jurídicas para licitud del tercero en el tratamiento de datos en el RGPD se deduce que actúa como una legitimación subjetiva a terceros y se presenta una nota crítica sobre esta cuestión (página 159).

ABSTRACT

The Thesis starts from the hypothesis of the existence of dysfunctions in the application of the General Data Protection Regulation (Regulation (EU) 2016/679, GDPR) in the field of healthcare. Said dysfunctions are detected both in what corresponds to the application of the General Data Protection Regulation in the procedural field, with the application of the principles, rights, and the legal basis itself that legitimizes the management of personal data, among others, and the application of said Regulation (EU) 2016/679 in the organizational field, especially in what refers to the implementation of the figure of the data protection officer, as a guarantee of the application of the General Data Protection Regulation itself. These dysfunctions have been highlighted during the process of managing the health alarm caused by the COVID19 pandemic and its conjunction with the respect for the fundamental right to the protection of personal data. During the course of the Thesis, these dysfunctions are especially analyzed in the public health sector of the Community of Madrid, being this analysis applicable to the Spanish public health sector, and legal solutions are provided to ensure the effective application of the GDPR.

The Thesis begins with the study of data in depth, which makes it necessary to define the concept of personal data or data on persons, in short, the factual element of the fundamental right that is protected. In this regard, data are that reality or fact captured by the human being which, once it is combined with another reality, is capable of providing information or conveying information about this reality. Data and information are not synonymous.

Personal data or data on a person provide information relating to an identified or identifiable individual, the rest is anonymous data. Since STS 6188/1996, the expression “data of personal character” has ceased to be used, instead the expression “personal data” is used. Regulation (EU) 2016/679 defines personal data as any information relating to an identified or identifiable natural person (“data subject”) and that, in the opinion of this Thesis, confuses data and information. It is not unusual for data to be confused with computer data, which is why the Thesis has deepened into the type of data subject to the GDPR, inferring that Regulation (EU) 2016/679 refers to any type of medium that may contain data and to any type of data that allows the identification of a person.

The GDPR and the Organic Law 3/2018 mention many types and sub-types of data; at least a list of thirty expressions that qualify the data and consequently differentiate them has been observed in Annex C. However, the GDPR basically defines two main types of data, data that fall within the scope of the GDPR and data that fall outside the scope of the GDPR. The group of data that fall within the scope

of the GDPR includes, on the one hand, those data qualified as special categories, which processing is prohibited except for exceptions, and, on the other hand, the rest of the personal data not included in these categories, which processing requires compliance with the legal bases of lawfulness. The special categories of data are ten, i.e., those of ethnic or racial origin, political opinions, religion or philosophical beliefs and trade union membership, as well as genetic data, biometric data, data concerning health, data concerning sex life or sexual orientation of a natural person. The Thesis stops at the data of ethnic or racial origin, because although it is included as a special category, the fifty-first whereas clause states that the European Union does not accept the existence of separate human races.

The protection of personal data corresponds to a fundamental right, both in Spain as an autonomous fundamental right independent of the right to privacy, based on Article 18 of the Constitution and STC 292/2000, and in the legal system of the European Union based on Article 8 of the Charter of Fundamental Rights of the European Union.

By referring to a fundamental right and by noting during the research process of the Thesis that some topics raise situations in which fundamental rights are in conflict with each other or with legally protected interests, it has led the Thesis to study the constitutional doctrine and the Constitutional Court in relation to this matter. In the year 2020 the WHO declared a health alarm of the COVID-19 pandemic; this situation caused the Government to activate the protocol for the establishment of the State of Alarm (Organic Law 4/1981 of June 1st), by Royal Decree 463/2020 of March 14th. The management of the pandemic has entailed the implementation of certain measures involving both the limitation of contact between individuals and the use of their personal data and personal data concerning health for the control of contagion and transmission of infection, bringing into conflict several fundamental rights, including the right to data protection and the right to free mobility and movement with the legally protected interests of health protection, showing, in turn, a clear lack of regulatory basis in Spain.

Once the legal concept of data and fundamental right has been dealt with, there is a discussion about the essential issues of the regulation of the fundamental right to the protection of personal data, which are undoubtedly the principles of data protection and data processing regulations and the rights that make possible the effectiveness of the application of the right to the protection of personal data.

The entire data processing activity consists of a succession of regulated actions to be carried out by data controllers and/or data processors, i.e. a procedure. The aim is to ensure that the decision-making process will be in accordance with the Law and, furthermore, that it will lead to a situation of balance in the interests of the data controller and/or data processor and the data subject, which, once again, leads us to an idea of material justice. Thus, we may state that adherence to this succession of actions will determine that the processing is lawful as well as fair.

If we want to outline the procedural stages of data processing, it would be as follows: Firstly, the means of processing must be determined and a prior risk assessment must be carried out; secondly, the basis for lawfulness of the processing must be specified, i.e., it must be determined whether there is a legal basis for such processing, under one of the assumptions of Articles 6 or 9 of Regulation (EU) 2016/679; thirdly, the data must be collected for specific, explicit and legitimate purposes; fourthly, the data must be recorded and stored, for which purpose the corresponding files will be created and a record of activity will be kept; fifthly, the actual data processing will be carried out, meaning any operation carried out on the data or set of data, in application of the principles and rights; and, finally, the data must be destroyed, either by erasure or by blocking.

This review of the essential procedural issues is necessarily complemented by a study of the institutions of control, regulation, processing, cooperation and self-regulation of the general data protection regulation. This description includes all the legal institutes of control and authority, supervisory authority, which regulate the application of the Regulation, bringing up two important tools of the supervisory body, namely, the act of implementation and the adequacy decision. Next, the description and functions of the three elements on which the principle of proactivity and the principle of self-regulation are based, namely the data controller, the data processor and the data protection officer, are discussed. These functions include the registration of activities, design protection and data security breach notification, as well as the personal data protection impact assessment projects of any processing and especially that of special categories and, based on the Thesis, the need to include the so-called Risk Maps. In this scenario, the Thesis focuses on the issue and describes the core aspects of the Regulation, namely: The purpose (the protection of personal data), the organization (the institutional structure), the functioning (guarantees and control) and the legal regime (rights and claims), supported by legal and doctrinal grounds on the nature of the regulation studied by the Thesis. This initial approach is followed by a specific consideration of data concerning health, which are especially protected, both in their strict interpretation and in the broad and extensive version referred to in the Regulation. The analysis of “data” is based on two pillars. Firstly, the processing to which personal data may be subject and the elements that compose them, i.e., basic, complementary, and additional elements, both when referring to personal data and to personal data in the health sector. Secondly, with regard to health, its three fundamental sources are described: The medical record, the prescription and the health card. The Thesis highlights the importance of the control of these data as they are subject to a certain vulnerability through the data called “personal identification code” which connects the medical record with the health card and the prescription. In other words, the processing of health-related data is carried out by combining two issues dealt with in the Thesis: On the one hand, the classification of the three elements of data processing and, on the other hand, the three fundamental pillars of personal data in the health sector, which are also understood in the Thesis as its data sources.

The study of personal data in the health sector has also been carried out from an organizational point of view, taking into account the health perspective, both the supervisory authority and the data controller and data processor, and finally the data protection officer, using as an example, in the latter case, the application of the General Data Regulation carried out by the Department of Health of the Community of Madrid and specifically the option of appointing a single data protection officer for all public healthcare centers.

The figure of the data protection officer and, more specifically in the public health sector, is dealt with in a comprehensive and complete way, once all the aspects that may influence it have been seen and analyzed. The designation and mandatory cases of designation set out in both Regulation (EU) 2016/679 and Organic Law 3/2018 are detailed. The Organic Law 3/2018 in its Article 34.1.L) determines the duty to designate a data protection officer in "Healthcare centers legally obliged to keep the medical records of patients". This obligation is also reflected in the disciplinary regime of the GDPR and especially in Article 73 of the Organic Law 3/2018 when it qualifies as a serious infringement "failure to comply with the mandatory designation of the data protection officer".

Actually, the figure of the data protection officer, firstly, must be approached from its nexus or connection with the Regulation, that is, from the figure of the data controller, since once this or, where appropriate, the processor hired by the controller is identified, and based on the nature of the organization and that of the necessary data, it is known where there is a duty to assign and designate a data protection officer. Secondly, it must be approached from its relationship with the object of the General Data Protection Regulation and the Organic Law 3/2018, that is, the protection of personal data and in this case, the protection of personal data in the health sector which includes the protection of the principles proclaimed by the GDPR and the rights to which the individual can avail himself/herself to make effective his/her fundamental right to protection of privacy and intimacy through the control of his/her data.

The study of the figure of the data protection officer has led the Thesis to analyze the application of the GDPR with regard to the Data Protection Officer (also, DPO) in the public health sector of the Community of Madrid. In 2018, the Department of Health created a Data Protection Committee replacing the DPO that each healthcare center must have, based on Organic Law 3/2018. The Thesis stops at Resolution PS/00417/2019 of June 9th, 2020 of the Spanish Data Protection Agency (AEPD) by which it sanctions company GLOVOAPP23, S.L. for serious infringement for not having a data protection officer despite the fact that the company claims to have a Data Protection Committee.

The Thesis could not and should not be closed without a constructive proposal that takes into account the complexity of the implementation of the GDPR and the intrinsic complexity of the health sector. Thus, it should be noted that the analysis of

the Thesis as a whole provides a pragmatic model that can be used by any national and/or regional administration for the proper application of the figure of the health protection officer in the public health sector.

This application model refers to the basic principles of the organization, which are: Analysis-detection, prioritization, design, control and participation of the parties involved. Finally, reference is made to one of the important aspects of the principle of proactivity and self-control, the creation of codes of conduct. The design of a manual for the application of the GDPR in the application sector is proposed as a consensual method and strategic basis, as a precursor to the creation of a code of conduct for the health sector.

Finally, a few comments in relation to some aspects criticized by the Thesis. During the preparation of the Thesis, partial findings and conclusions are made on specific issues that affect some of the topics dealt with. In this scenario, when studying data, a "critical note" (page 33) stands out in relation to the fact that the GDPR confuses the concept of data and information, which are not synonyms.

It is discussed in a "critical note" (page 239) that the GDPR mentions that adherence to a Code of Conduct is synonymous with demonstrating the existence of appropriate safeguards, when this adherence only demonstrates the intention of the adhering party, but not compliance.

At the time that the Thesis addresses the issue of the response of the health system to the demand for care created by the pandemic, it has become clear that the Public Health Surveillance Network required by Article 13 of Law 33/2011 is not in place yet (as of 04/30/2021) and the National Epidemiological Surveillance Network created in 1995 continues operating (page 167). Furthermore, on page 167 through a "critical note" it is deduced that in Spain, after the first months of management of the pandemic, an Organic Law should have been passed which will regulate the adoption of the necessary measures regarding the processing of personal data to be adopted by the Government and the Administration; measures which will have to respect the minimum guarantees contained in the GDPR.

In a "critical note" (page 318), the Thesis disagrees with the fact that the AEPD understands that health professionals are not obliged to request consent from patients for the collection and use of personal and health data.

Regarding innovations to be highlighted. The Thesis studies data processing reflected in the referred regulations, inferring that they include many actions or operations and that once ordered, a new classification arises, organized on the basis of their components, which are the basic elements of processing, the complementary and additional ones. This classification is applied to health-related data in each of their three main sources: The medical record, the prescription and the health card. On the other hand, the lawfulness of data processing is studied both in its general and health aspects and, based on the general theory on ordinary and extraordinary legitimacy,

the types of legitimacy appearing in the GDPR are described. These are the subjective legitimacy and the objective legitimacy. The treatment of professional secrecy as one of the legal bases for the lawfulness of the third party in data processing in the GDPR leads to the conclusion that it acts as a subjective legitimacy to third parties and a critical note on this issue is presented (page 159).

PRESENTACIÓN

Esta Tesis arranca de la hipótesis de la existencia de disfuncionalidades en la aplicación del Reglamento (UE) 2016/679 en un ámbito tan sensible como el sanitario, las cuales se presentan tanto en lo procedimental (bases jurídicas, principios, derechos, entre otros) como en lo organizativo (delegado de protección de datos como garantía de su aplicación). Se utiliza el caso de la Consejería de Sanidad de la Comunidad de Madrid como ejemplo práctico. En opinión de esta Tesis el Servicio Madrileño de Salud ha aplicado incorrectamente el Reglamento (UE) 2016/679 del Parlamento 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 (RGPD) y a la libre circulación de estos datos y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en cuanto se refiere al delegado de protección de datos.

Esta Tesis confirma la hipótesis del investigador, es decir, el RGPD está insuficientemente implantado en el sector público de la salud, utilizando como ejemplo el caso de la Comunidad de Madrid pues no es correcta la opción adoptada y que se comunicó el 27 de abril de 2018 en relación a la política de designación de delegado/s de protección de datos en todo el conjunto de centros dependientes de la Consejería de Sanidad y del SERMAS y más en concreto la decisión de "el nombramiento del Delegado de la Consejería de Sanidad en la figura colegiada del Comité Delegado de Protección de Datos.", dejando, a su vez, los centros sanitarios sin delegados de protección de datos.

Para el estudio de la hipótesis se ha investigado tanto en el Reglamento (UE) 2016/679 como en la Ley Orgánica 3/2018 y en toda la legislación relacionada la esencia y contenido real del tratamiento de datos personales relativos a la salud y en especial los lugares y las fuentes de dichos datos. Se ha utilizado la jurisprudencia del Tribunal Constitucional, la de Tribunal Supremo, la de algunos Tribunales Superiores de Justica, así como la del Tribunal de Justicia de la UE.

La Tesis se nutre de los documentos emitidos por la AEPD y por los organismos públicos españoles y de la Unión Europea. Además, se nutre de otras fuentes nacionales e internacionales.

El desarrollo de la Tesis empieza en su Título I, régimen básico, analizando el Reglamento (UE) 2016/679 como en la Ley Orgánica 3/2018 en todos aquellos puntos que pueden afectar tanto al dato, como al tratamiento del mismo y a toda la estructura o escala jerarquía que ejerce el control y desarrollo de la política de protección de datos personales dentro de la Unión Europea y en especial en España. Se tratan los principios sobre los que se basa el Reglamento General de Protección de Datos, los derechos que crea y hacen posible la efectividad del derecho a la protección de los datos personales. Este Título I analiza de forma pormenorizada el tratamiento de datos con carácter general, la licitud para el tratamiento de los datos protegidos y finaliza dedicando un apartado al tratamiento de datos personales en la gestión de una alarma sanitaria.

El análisis de Título I incorpora una nueva lectura del contenido y del alcance de la expresión "tratamiento de datos", esta nueva calificación se refiere a los elementos básicos del tratamiento, de los elementos complementarios del tratamiento y de los elementos adicionales en el tratamiento de los datos personales. En el capítulo 5.4 se trata la cuestión de las bases jurídica para la licitud del tratamiento de datos personales, descriándose la legitimación subjetiva indirecta.

El Título II describe las instituciones de control, regulación, tratamiento, cooperación y autorregulación en el contexto del RGPD. Se inicia con unos capítulos dedicados a los órganos de control y a la Autoridad de control en los Estados Miembros de la UE. Se guie con un capítulo dedicado a responsable y encargado del tratamiento de datos en el RGPD y siguiendo con un capítulo para el delegado de protección de datos. El capítulo 5 de este Título II trata de la autorregulación en el RDPG y finalizando con un capítulo para los mecanismos de cooperación y coherencia dentro del RGPD.

El Título III, régimen de protección de datos relativos a la salud y en el ámbito sanitario, aplica todos los elementos del régimen básico al tratamiento de los datos personales relativos a la salud y ámbito sanitario, explicando, en primer lugar, con mucho detalle el objeto y ámbitos materiales en los que se desenvuelve tanto el dato relativo a la salud como el dato en el sector sanitario susceptible de ser tratado como dato relativo a la salud. Es decir, aquel dato sobre la salud de las personas susceptibles de ser protegidos por el RGPD y aquellos otros datos que sin ser datos de salud acaban siendo tratados con el mismo régimen de protección, bien por el ámbito en el que se han generado o recogido o bien por la persona que ha accedido a los mismos de forma voluntaria o involuntaria.

El Titulo III incluye además de la historia clínica, del artículo 34.1.i) de la Ley Orgánica 3/2018, otros dos soportes que dan cabida al dato de salud, estos son la receta sanitaria y la tarjeta sanitaria, soportes afectados por el RGPD.

El Titulo III se cierra con el análisis con el capítulo 6.3. que hace referencia al caso práctico o ejemplo utilizado para ver la incorrecta utilización que se puede hacer en la sanidad pública del RGPD y en concreto de la figura del delegado de protección de datos en la Comunidad de Madrid desde la entrada en vigor del Reglamento (UE) 2016/679 y desde la entrada en vigor de la Ley Orgánica 3/2018.

El Título IV, inicia todo el contenido en la identificación de la figura del responsable del tratamiento de datos personales relativos a la salud. El capítulo 2 sigue con el análisis del papel de delegado de protección de datos tanto en la protección de los principios del RGPD como en la aplicación de los derechos que emanan del RGPD, en el sector público de la salud. El capítulo 3 se centra en analizar el papel del delegado de la protección de datos en todo el tratamiento de datos en base al capítulo 1.2.4 del Título III. Finalmente, este Título concluye con el papel del DPO en la gestión de los datos en una pandemia.

EL Titulo V "Una propuesta para la correcta aplicación de la figura del delegado de protección de datos en el sector público de la sanidad en España" tras todos los pasos

que ha seguido la Tesis, tras todas las conclusiones a las que ha llegado capítulo tras capítulo se presenta un Modelo para la aplicación de la figura del DPO en la sanidad pública de cualquier reunión de Europa. En modelo empieza en el capítulo 1, mediante un simple estudio de campo para conocer el escenario que hay que tratar y en segundo lugar, en función del punto anterior se proponen los DPO necesarios, su forma de coordinarlos y los documentos que recoge tanto el espíritu como el articulado del RGPD.

Finalmente, la Tesis finaliza con las Conclusiones. Estas conclusiones se presentan de dos formas. En primer lugar, las conclusiones globales, que reflejan capitulo por capítulo la conclusión del mismo. En segundo lugar, las conclusiones finales, que resaltan en algo mas de una decena de conclusiones a las que llega la Tesis.

El documento contiene una serie de **Notas Cítricas**: la confusión entre dato e información, capítulo 1.3 del Título I; el secreto profesional como único y principal elemento legitimador de terceras personas para el tratamiento de los datos relativos a la salud, capítulo 3.5.3 del Título I; “la naturaleza de la adhesión a un código de conducta”, del artículo 32 del Reglamento (UE) , capítulo 8.1 del Título I: “desde el año 2011 se está esperando que las AAPP creen la Red de Vigilancia de Salud Pública; AEPD y la exclusión del consentimiento capítulo 3.2.1. del Título III; y AEPD y la exclusión del consentimiento el capítulo 5.1.2. del Título III.

TÍTULO I. RÉGIMEN BÁSICO DE LA PROTECCIÓN DE DATOS

Capítulo 1. Concepto jurídico de dato

1.1. Cuestiones preliminares

Con carácter preliminar se realiza en pequeño y breve análisis de la voz "dato" y en qué forma y manera es utilizada semánticamente por las normas que competen al RGPD en España, realizando, a su vez, una comparación de la utilización de la voz *dato* en ambas normas ([Anexo A]), es decir, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales .

La ley no define al dato, como se verá en capítulo 1 del Título I, por lo que deberá ser a través del análisis semántico de la norma lo que permita al lector hacerse una idea de lo que la ley entiende por ese concepto. A los efectos de conocer lo que presupone la Ley orgánica por dato, se han analizado las distintas formas de utilizar el vocablo dato por parte de ambas normas.

Para buscar el significado de las palabras hay varias formas. Esto es, bien analizando el significado que las Academias de la Lengua dan a las palabras o bien viendo cómo y de qué manera se utilizan. Es decir, si la ley no define el concepto, entonces podremos deducir su significado viendo de qué forma y manera utiliza la ley dicha palabra. Las dos normas sobre que la Tesis investiga, en este sentido, son las que regulan el tratamiento del dato personal, por una parte, el Reglamento (UE) 2016/679 y por otra parte la Ley orgánica 3/2018.

Las normas a estudio, al hablar de los datos como algo que se puede usar (uso de sus datos o utilización de los datos) entienden que son cosas materiales o inmateriales que tiene un uso o una utilidad para la sociedad, además al utilizar la expresión, usar, demuestra que además de usarse se pueden utilizar, tal como si se tratara de cosa útil. Además, si bien los datos se entienden como algo que se puede usar o utilizar y también se debe entender como algo a lo que se puede acceder (acceso a los datos), por ejemplo, la expresión del RGPD "acceso a los datos y documentos de la historia clínica".

La norma entiende que el dato no es tal sino sufre un proceso de anotación o registro (registro completo de los datos), de tal forma que un dato no registrado no se afectaría por ninguna de las dos normas. También entiende que el dato puede ser soportado por cualquier soporte (tratamiento total o parcialmente automatizado de datos personales) y no exclusivamente por uno solo de ellos.

A las expresiones sobre datos que hemos señalado, se puede añadir que las normas tienen en cuenta el dato y su cantidad (cantidad de datos) ("datos personales a gran escala") ("tráfico masivo de datos personales"), así, pues es algo medible. Además, también se refieren al dato como algo que se puede mover de un lugar a otro ("libre

circulación de estos datos, portabilidad de los datos") o incluso pueden ser comunicados ("comunicación de datos"), movilidad inmaterial. Además, los datos se pueden categorizar ("categoría especial de los datos", categorías de datos objeto de tratamiento) y ver su condición en relación a las personas, de aquí los datos personales ("datos personales") y, en consecuencia, los datos no personales. A su vez, la norma entiende que trata de datos personales pero que también se categorizan en función de la capacidad de la persona, así pues, en base a su mayoría de edad (datos de menores de edad) o vigencia (tratamientos de datos de personas fallecidas).

Las normas utilizan la palabra dato como elementos o cosas que pueden ser anonimizados o seudonimizados, lo cual significa que estos a efectos de la norma son nominales ("reidentificación de los datos"); y pueden ser bloqueados, lo cual atiende tanto a una justificación suficiente como a su relevancia e importancia. Esta importancia hace que la norma entienda que el dato y su tratamiento requiera de un responsable ("responsables y encargados del tratamiento de datos"). Esta importancia se resalta al ponerle el velo protector de la confidencialidad o reserva ("confidencialidad de los datos") y sobre todo al referir el dato a un derecho fundamental ("derecho fundamental a la protección de datos") y concretamente al derecho fundamental de la protección de la intimidad. La norma presupone que el dato es un elemento que a falta de una norma de máximo rango está por si solo desprotegido al hablar de su protección ("protección de datos") ("protección de datos personales") ("seguridad de los datos personales"). Por tanto, dato personal es equivalente a intimidad, pues la intimidad sin norma que la proteja es un factor o cosa con un alto riesgo de ser dañado o vulnerado.

De tal suerte, que la norma trata al dato como una cosa o elemento que merece tanta protección que incluso se puede prohibir su conocimiento ("prohibición del tratamiento de datos").

También se le entiende como cosa concreta ("datos concretos") y, en consecuencia, también los habrá inconcretos, de lo cual se deduce que la concreción o no de los datos es motivo suficiente como para que se tenga en cuenta. A su vez además de la concreción se entienden como cosas que pueden ser inexactas ("datos inexactos") y, en consecuencia, también cosas exactas ("datos serán exactos", "exactitud de los datos"). La norma se refiere al dato como un elemento material, pues la supresión o rectificación alude a cosa material ("rectificación o supresión de datos personales"). Los datos pueden ser censados ("datos censales") y pueden tener fines públicos ("datos con fines de archivo en interés público").

En este orden de cosas, datos son elementos que se pueden o deben conservar ("conservación de datos") ya sean estos bloqueados ("conservación de los datos bloqueados"), identificativos o que identifican ("conservar los datos identificativos") y que, a su vez, se pueden o deben controlar ("control sobre sus datos", "control sobre sus datos personales"). Así pues, datos son cosas que se puede destruir o conservar ("destrucción de los datos").

La norma insiste en que los datos son cosas que pueden ser facilitadas ("datos que hayan sido facilitados") o en sensu contrario, cosas a las que se puede acceder sin ser facilitadas, bien porque son obtenidas ("datos obtenidos") o bien porque son facilitadas. También, datos como cosas necesarias ("datos necesarios") y, en consecuencia, los habrá no necesarios o innecesarios.

Los datos también son cosas que pueden ser reflejo de obligaciones, tal es lo penal ("datos relativos a la comisión de infracciones penales o administrativas"), fiscal ("datos tributarios") o lo crediticio ("datos se refieran a deudas ciertas"), ("datos referidos a un deudor", "sistema de información crediticia con datos relativo" o "puesta a disposición de los datos a los jueces y tribunales").

Las normas apelan al "fin del dato" o más aun al fin del tratamiento del dato, íntimamente vinculado al fin del propio dato ("tratamiento de datos con fines de archivo") ("tratamiento de datos de contacto") ("tratamientos de datos de salud") ("tratamiento de datos de la investigación en salud") ("tratamiento de datos de naturaleza penal") ("tratamiento de datos en el ámbito de la función estadística pública") ("tratamiento de datos relativos a infracciones y sanciones administrativas") ("tratamiento de los datos personales procedentes de las imágenes y sonidos").

Dos de las expresiones más debatidas y sobre la cual el Tribunal Supremo Español tomo posición son "datos personales" y "datos de carácter personal". En este sentido el texto articulado del Reglamento 2016/679, tan solo utiliza en dos ocasiones la expresión "datos de carácter general", mientras que en 19 ocasiones utiliza la expresión "datos personales". La Ley Orgánica 3/2018, utiliza la expresión "datos personales" en 84 ocasiones dentro de su articulado, mientras que "datos de carácter personal" solo la utiliza al referirse a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.2. El dato

De la lectura de los textos legales relativos a la protección del dato, surge la pregunta ¿esta protección qué protege? Y la respuesta es, protege un derecho fundamental cuyo soporte fáctico es el dato. Es decir, el dato es el objeto de protección como expresión de la intimidad. A continuación, nos surge la pregunta de ¿qué es el dato y qué significa "tratamiento de datos"?, y en el supuesto de que hubiera varios tipos de datos ¿qué tipo de dato protege?, ¿quién es el sujeto pasivo de esta protección? Y sobre todo ¿qué es el dato para la ley que lo protege?

En la sociedad actual y en las bases de su funcionamiento se sitúa todo el contexto del dato y de la información que este suministra. No se concibe el funcionamiento de las instituciones, personas jurídicas y de las familias sin la existencia de los datos y de la información. Nace el dataismo como aquella teoría mediante la se explica que la realidad se convierte en datos[1].

[1] SERRAT ROMANI, M. (2017) "Los derechos de los contribuyentes en un entorno digital". Revista Privacidad y Derecho Digital, 7, 67-107. Año II. p 73.

En un entorno que se circunscribe a la protección del dato es del todo preciso concretar, en la medida de lo posible, lo que se entiende por dato en un sentido amplio y en un sentido concreto. Para la RAE dato deriva del latín *datum*, lo que se da, además, dice que es información o, incluso, documento, brindándonos poca, o ninguna, ayuda.

Dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, visual, etc.) de un atributo o variable cuantitativa o cualitativa, es decir, el valor que toma cada una de estas[2]. Un dato aislado no tiene más sentido que la magnitud que representa, es un elemento neutro, es expresión básica o expresión mínima básica del contenido del conocimiento, es una expresión simbólica o un valor dado a una realidad o una cosa. Cuando un dato se referencia, activa o pasivamente, a otro dato entonces ambos expresan o significan algo más que la mera magnitud de cada uno por separado. Otra forma sencilla de acercarse al concepto de dato es presentarlo como un reflejo de la realidad, en el sentido de que para determinados autores el dato conforma una realidad absoluta, solamente contrastable con más datos[3].

El Convenio 108, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, no define el término dato[4]. Si bien el término dato está definido en las Leyes de Irlanda y Reino unido, relativas a la protección de datos tampoco consiguen una definición concreta y útil[5].

En este sentido, el dato ha sido definido como un identificador, al referirse al dato de una persona que la identifica como tal. Esta nueva expresión al referirse a un dato, aparece en el apartado 1 del artículo 4 del Reglamento (UE) 2016/679 al decir que “dato personal es aquel que funciona como un identificador”.

[2] PITA FERNÁNDEZ S., PÉRTEGA DÍAZ S. (2001) “Estadística descriptiva de los datos”, Atención primaria en la red. 8: 37-41. p 2.

[3] SERRAT ROMANI, M. (2017) “Los derechos de los contribuyentes …..”, op.cit; p 73.

[4] CONSEJO DE EUROPA (1981) “Convenio 108 del Consejo de Europa, de 28-1-1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal”, hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España el 27 de enero de 1984 (entró en vigor de forma general el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo). (BOE núm. 274 de 15-11-1985). Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447 (31/05/2020).

[5] La autora, LAZPITA GURTUBAN, nos demuestra que las dos leyes mencionadas tampoco aciertan en cuanto a la definición de dato, repitiendo la habitual confusión entre dato e información. De tal forma la autora nos dice: “Ambas leyes lo hacen de forma diferente siendo la definición británica más restringida que la irlandesa, "Data" es definido en el Reino Unido como "toda información, registrada de manera, que pueda ser procesada por un equipo que opere automáticamente en respuesta a las instrucciones que se le hayan dado para dicho propósito". El hecho de incluir la palabra registrada (recorded) limita el alcance de la definición. La ley irlandesa habla de "La información que pueda ser procesada" y abre el alcance de la ley a nuevas aplicaciones tecnológicas.” LAZPIRA GURTUBAN M. (1994) “Análisis comparado de las Legislaciones sobre Protección de Datos de la Estados miembros de la Comunidad Europea”. Revista Informática y Derecho, 6 y 7, 397-420. pp 397 y ss.

En base a las teorías de la investigación y siguiendo a Gil Flores[6], se puede definir el dato como aquella información extraída de la realidad que tiene que ser registrada en algún soporte físico o de símbolos, que implica una elaboración conceptual y además que se pueda expresar en algún tipo de leguaje.

Un conjunto organizado de datos procesados y ordenados da información, constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje[7]. La información está constituida, pues, por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje[8]. Cuando la información se almacena mediante la experiencia o el aprendizaje o mediante técnicas de introspección u observación, esta genera conocimiento. El conocimiento es la elaboración abstracta de nuevos conceptos e ideas producto de la información y la experiencia, pero la información no es equivalente a conocimiento[9].

Sin embargo, hay entidades especializadas en el tratamiento de la información que entienden que la información es posterior al conocimiento y no previa a él. Así la Oficina Nacional de Seguridad del Centro Nacional de Inteligencia entiende que "información es todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma"[10].

La información, la tecnología y el aprendizaje han sido los gérmenes que han contribuido a hacer del conocimiento un verdadero factor de producción en el mundo de hoy. Dato, información y conocimiento forman los tres eslabones de esta máquina productiva[11]. Cuando el dato se organiza y comunica se transforma en información[12]. Esta función del dato que adquiere al ser ordenado o valorado conjuntamente con otros datos convirtiéndose en una función de información aparece en muchas sentencias, sin ir más lejos en el cuarto Considerando, de la página tres de la Sentencia del Tribunal Supremo de 30 de octubre de 1978 cuando dice "……y todos estos datos, conjuntamente valorados, fundamentan como mínimo……."[13].

Un símil de la relación entre dato e información se puede constituir utilizando el lenguaje de la música, esto es, la relación entre los sonidos de la escala diatónica, el pentagrama y la música. Una nota musical o sonido de la escala diatónica en sí mismo no es más que

[6] GIL FLORES J. (1994) "Análisis de datos cualitativos. Aplicación a la investigación cualitativa". Barcelona. Edit. PPU. Cap 1. Universidad de Murcia. Disponible en www.um.es/docencia/pguardio/documentos/Tec3.pdf (31/01/2021) p 180.

[7] BURNINGHAM, D., BENNETT, P., CAVE. M., HERBERT, D., HIGHAM, D. (1988), "Economía". Madrid. Ediciones Piramide. pp34-36, 200-203.

[8] RODRÍGUEZ GÓMEZ, D. (2006) "Modelos para la creación y del conocimiento: una aproximación teórica". Educar. 37, 25-39.

[9] QUADRA SALCEDO T., PIÑAR MAÑAS JL. M. BARRIO A., TORREGROSA VÁZQUEZ J., (2018) "Sociedad digital y derecho". Ministerio de Industria, Comercio y Turismo. Madrid. Boletín Oficial del estado. p 172.

[10] ONS. "Protección de la información clasificada". Disponible en https://www.cni.es/comun/recursos/descargas / DOCUMENTO_1_-_Principios_bxsicos_ proteccixn_IC.pdf. p 1.

[11] MARSHALL A. (1890) "Principles of Economics: an introductory text". Reimprison 2013. pp170-174

[12] ŻELAZNY, R. (2015) "Information Society and Knowledge Economy, Essence and Key Relationships". Journal of Economics and Management. Vol 20 (2), 5-22. p 7.

[13] STS 6804/1978 de 30 de octubre (Sala de lo Contencioso), Considerando 4º.

un sonido, equivaldría a un dato. Existen siete distintos sonidos estos son: do, re, mi, fa, sol, la, si. Cuando las notas musicales, en base a las claves, se asocian en un determinado orden surge lo que se entiende por música, equivaldría a información. Es decir, un ejemplo de la cadencia entre el dato y la información.

Otro símil se da entre la relación de las letras del abecedario y las palabras. Sin duda, una consonante aislada o una vocal aislada no tienen ningún significado, en general. Sin embargo, muchas letras una detrás de la otra correctamente ordenadas, dan contenido a una frase, a un párrafo y aun texto completo. Es decir, frente a la elementalidad del dato, vocal, se sitúa la complejidad de la información, frase.

Sin embargo, la confusión entre dato e información está muy extendida. La Ley irlandesa relativa a protección de datos, muy genérica, entiende que dato es equivalente a información, a la que puede ser procesada, mientras que la Ley del Reino Unido, más extensa, incurre en la misma confusión diciendo que dato es toda información registrada de manera que pueda ser procesada[14].

El ordenamiento jurídico español define en varios textos lo que entiende indirectamente por dato. Es habitual que se confunda el concepto de dato con el concepto de información, tal es el caso de la ley 41/2002 que define como Información clínica a todo dato, cualquiera que sea su forma, clase o tipo, que permita adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla.

Se observa que las definiciones utilizan alternativamente el concepto de dato y el concepto de información, utilizando a uno para definir al otro. Lo cierto es que, si bien están íntimamente ligados, datos e información no son en su esencia sinónimos. Está claro que sin datos no hay información, pero también es cierto que no todo dato es información o es capaz de generar información. El dato 170 en sí mismo no significa nada, cuando se adjunta a este dato el dato “centímetros”, entonces, adquiere un significado y cuando se adjunta a estos dos datos el dato “persona”, entonces entendemos que es una información relativa de la estatura de una persona.

De esta forma, entendemos que el dato por sí solo no aporta nada, sino que cuando un dato se relaciona con otro o con un contexto, adquiere importancia pues este transmite información y esta información puede corresponder a una persona. En este orden de cosas, el dato es cualquier representación simbólica que emana de la realidad o de un hecho, por tanto, identificativa, que al juntarse o sumarse en el tiempo a otro dato desvele información sobre algo o alguien, permitiendo llevar a cabo una imagen o idea mental una realidad de algo o alguien.

[14] LAZPIRA GURTUBAN M. (1994), (1994) “Análisis comparado …..”, op.cit; pp 397 y ss.

Si bien poco hay que añadir a la relación entre dato e información, hay que destacar que el dato tiene valor en relación al contexto en donde se emita. De esta forma un simple dato como es el registro contable se configura como un registro jurídico con eficacia[15].

En el sector público hay un elenco normativo que de una forma directa o indirecta alude al dato y a su naturaleza. De tal forma la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno en su preámbulo distingue entre dato e información subordinando el segundo al primero "….. se incluyen datos sobre información institucional, organizativa y de planificación, de relevancia jurídica y de naturaleza económica, presupuestaria y estadística".

Así pues, no debe asociarse por el término *dato* a un concepto que transmite banalidad, tal como hacen expresiones corrientes tales como "es solo cuestión de datos", sino que dato debe entenderse como el componente más elemental de la relación humana en su contexto social. Otro símil, dato correspondería uno de los miles de ladrillos que componen al ordenarlos una construcción arquitectónica en su conjunto.

La importancia del dato y de la información también se transmite a la necesidad de gestionar con eficacia tanto el dato como la información y evitar los efectos negativos de la sobrecarga de información[16], es decir, evitar la mala gestión del dato, ver por ejemplo el artículo 5 del Reglamento (UE) 2016/679.

En conclusión, no en vano la importancia de dato ha provocado su protección al máximo nivel dentro del Estado de Derecho, de esta forma queda constancia con el Reglamento (UE) 2016/679 de la UE y con la Ley Orgánica 3/2018.

1.3. Dato personal

En el punto anterior se ha tratado de definir lo que se entiende por dato, llegando a la conclusión de que es cualquier representación simbólica que emana de la realidad o de un hecho[17], por tanto, identificativa, que al juntarse o sumarse en el tiempo a otro dato desvela información sobre algo o alguien, permitiendo llevar a cabo una imagen o idea mental de una realidad de algo o de alguien.

No todo dato tiene la misma relevancia o importancia, siendo los datos más relevantes aquellos que pueden generar derechos y obligaciones y sobre todo aquellos que están vinculados a las personas, a su realidad y a su identificación. En este orden de cosas los datos de las personas que no permiten bajo ninguna circunstancia la identificación de una de ellas, si bien gozan de su esencia propia apenas tienen relevancia jurídica. Es el propio Reglamento (UE) 2016/679 que muestra esta relevancia al establecer su objeto,

[15] NAVARRO RUIZ, G. (2019) "Aplicación de la tecnología blockchain a emisiones de valores negociables". Revista Privacidad y Derecho Digital, 15, 127-170. Año IV. p 137.

[16] KOONTZ, H., WEIHRICH. H. (1990), "Administración". México. Ed. McGraw-Hill. pp 536-538.

[17] "Según las normas comunitarias y nacionales de protección de datos se entiende como "cualquier información" tanto información objetiva, como las evaluaciones subjetivas, estén o no probadas. De igual forma, se considera que los datos pueden aparecer en forma alfabética, fotográfica, sonora o cualquier otras (Gil, 2016)" MORENO ZAMBRANO V. (2019) "Minería de datos en plataformas de entretenimiento de cara al RGPD". Revista Privacidad y Derecho Digital, 13, 157-168. Año III. p 163.

artículo 1.1., el establecimiento de "las normas relativas a la protección de las personas físicas en lo que respeta al tratamiento de los datos personales".

La relación de la persona física (o persona jurídica) y los datos es íntima e indisoluble[18]. Los datos si bien existen por sí solos, es la persona, su actividad y su interrelación con los demás lo que les da naturaleza y utilidad. Los datos adquieren en la relación humana un papel extraordinario y en especial en el ámbito jurídico de la misma, no en vano el ordenamiento jurídico vincula los derechos y las obligaciones de las personas a los hechos y a los actos y estos a su vez a su conocimiento, consentimiento, efecto y eficacia, todo ello bajo el paraguas de su constatación y que en definitiva esta se da mediante datos e información. Es decir, sin dato no hay relación jurídica.

Sin embargo, esta dimensión universal del dato contrasta con el contexto singular y parcial que algunos autores le dan al dato, de esta forma llama la atención expresiones como la de "economía de datos" al referirse a la actividad económica de todo el mercado del dato digital, de tal forma que se estima que este concepto abarcar a 300 billones de euros en el año 2016 en la Unión Europea[19]. En este orden de cosas, la Comisión Europea remitió una Comunicación al Parlamento Europeo sobre la construcción de una economía de los datos europea, en la cual hace constar "La economía de los datos se caracteriza por un ecosistema en el que diferentes tipos de agentes del mercado –como fabricantes, investigadores y proveedores de infraestructuras– colaboran para garantizar que los datos sean accesibles y utilizables. Esto permite a dichos agentes extraer valor de esos datos, creando toda una gama de aplicaciones con un gran potencial para mejorar la vida cotidiana (por ejemplo, la gestión del tráfico, la optimización de las cosechas o la atención sanitaria a distancia)"[20].

La gran importancia que la sociedad occidental a la información, y por ende al dato, se basa precisamente en la necesidad que tiene la sociedad de generarla para que la esencia de la persona y el efecto de las relaciones entre personas tengan sus efectos y legitimidad. De esta forma en la sociedad la relación del dato y la persona es indisoluble.

Así pues, lo que es bueno para la persona, es decir, estar en posesión de datos e información contrastable, verídica y demostrable también puede ser malo para la misma persona, es decir, que estos datos o información vayan en contra de sus derechos o perjudiquen o comprometan el pleno desarrollo presente o futuro de los mismos. De esta forma, es el propio Reglamento (UE) 2016/679 el que tiene como objeto, en su artículo 1.2, proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

[18] MURILLO DE LA CUEVA, PL. (1999) "La construcción del derecho a la autodeterminación informativa". Revista de Estudios Políticos (Nueva Época), 104, 35-60. p 35.

[19] ORTIZ LOPEZ, P. (2018) "Los datos personales. ¿Una propiedad o un derecho fundamental?". Revista Privacidad y Derecho Digital, 10, 179-182. Año III. p 179.

[20] COMISIÓN EUROPEA (2017) "La construcción de una economía de los datos europea". Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Disponible en https://eur-lex.europa.eu/content /news/ building_ EU_data_economy.html?locale=es (28/02/2021).

Esta íntima relación entre las personas y los datos y la información y más cuando estos datos son o hacen referencia a cuestiones íntimas de las personas ha provocado que las legislaciones de los países, que sustentan sus sistemas en Estados de Derecho, se ocupen de su protección y más aún se interesen en proclamar derechos especiales sobre determinada información tal es el caso de la información generada por los actos de naturaleza sanitaria o relacionados con la salud de las personas[21].

La Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos, ofrece una definición de dato personal que versa sobre que la expresión *datos personales* y abarca cualquier información relativa a un individuo identificado o identificable. Un individuo no se considerará "identificable" si la identificación requiere una cantidad de tiempo y de medios no razonables. En los casos en que el individuo no sea identificable, los datos son denominados anónimos.

La Ley 14/2007, de 3 de julio, de investigación biomédica entiende por dato anónimo como aquel dato registrado sin conexión o nexo con una persona identificada o identificable.

El Reglamento (UE) 2016/679 en su artículo 2.2.c) hace referencia a que el ámbito doméstico queda excluido de la aplicación del RGPD, lo cual conlleva a decir que los datos personales en este ámbito no están incluidos, a lo cual el TJUE entiende que solo incluye las actividades de la vida personal y familiar de los particulares, lo cual no incluye la utilización del internet en el domicilio personal[22].

Las expresiones datos personales y datos de carácter personal se utilizan en el ordenamiento jurídico, basta con observar la denominación de la Ley de 1999, ya derogada, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Sin embargo, tal como veremos el ordenamiento jurídico español en la Ley Orgánica 3/2018 ha dejado de utilizar la expresión "datos de carácter personal".

Si bien la Ley Orgánica 3/2018 ya no utiliza la expresión "datos de carácter personal" el ordenamiento jurídico en su conjunto utiliza indistintamente la expresión datos personales y datos de carácter personal, como ejemplo de ello son: artículo 56.3 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud; artículo 54.2 de la Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios; artículo 3 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos; artículo 28.4 y 28.5 del Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso; artículo único.nueve del Real Decreto 1302/2018, de 22 de octubre, por el que se modifica el Real Decreto 954/2015, de 23 de octubre, por el que se regula la indicación, uso y autorización de dispensación de medicamentos y productos sanitarios de uso humano por parte de los enfermeros.

[21] RULE JB., GREENLEAF G. (2008) "Privacy Protection: The First generation", USA. Edward Elgar. pp 4-6.
[22] STJUE de 6 de noviembre de 2003 (Sala primera) (asunto C-101/01) apartado 4, p I-13014.

Pero tal como dice el Tribunal Supremo, que si bien son casi lo mismo no son sinónimos uno del otro.

El Tribunal Supremo aborda esa cuestión en la STS 6188/1996, de 31 de octubre del 2000. La sentencia del Tribunal Supremo cuyo ponente es el Sr. Francisco González Navarro, dice[23]:

> "no siempre un dato personal es un dato de carácter personal, y porque, además, hay datos de carácter personal que no son datos personales.
>
> En principio, los datos de carácter personal son de tres clases:
>
> a. Datos personales stricto sensu, que son aquellos datos existenciales que pueden ser asociados a una persona determinada o determinable (nacimiento, muerte, matrimonio, domicilio, y análogos), los datos referentes a la actividad profesional, al patrimonio, a la pertenencia a una confesión religiosa, a un partido político, las enfermedades, etc.
>
> b) La "La información sobre las condiciones materiales", concepto que quedaría englobado dentro de la ambigua frase empleada por el artículo 3, letra a) LORTAD: "cualquier información".
>
> c) Evaluaciones y apreciaciones que puedan figurar en el fichero y que hagan referencia al afectado.
>
> Pues bien, desde el punto de vista de la protección de que gozan los datos de carácter personal -y, consecuentemente, la persona concernida o afectada por los mismos- los datos de carácter personal son de dos clases: datos accesibles al público y datos no accesibles al público. De la primera clase son aquéllos que aparecen recogidos en bases de datos públicas, tales como repertorios de jurisprudencia, listas telefónicas, etc. y cuya publicidad no éste vetada o restringida por ninguna norma limitativa (para más detalle cfr. Art. 1.3 del Real decreto 1332/1994, de 20 de junio)."

La Ley Orgánica 5 / 1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, derogada en 1999, definía "datos de carácter personal" como "cualquier información concerniente a personas físicas identificadas o identificables". La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, derogada por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales, definía dato de carácter personal a "cualquier información concerniente a personas físicas identificadas o identificables", idéntica a la Ley Orgánica 5/1992 a la cual deroga, sin embargo, la Ley Orgánica 3/2018 no aporta definición alguna sobre el dato personal.

En el reglamento, Real Decreto 1720/2007 de 21 de diciembre de 2007, de la Ley Orgánica 15/1999 (derogada) en su artículo 5 f), dice que: "Datos de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". En su artículo 5 g) dice:

> "Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se

[23] STS 6188/1996 de 31 de octubre (Sala de lo Contencioso), FD 2º.

> consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética".

Aunque de forma tan solo indirecta, podemos acudir a la Ley 14/2007, de 3 de julio, de investigación biomédica para ver como el legislador entiende el significado del dato personal de tipo genético. De tal forma el artículo 2 de esta Ley entiende por dato genético de carácter personal, aquella información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos.

El propio Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 introduce una definición de los datos personales ampliando las anteriormente conocidas:

> "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

En base a este Reglamento, como datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo:

> "todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

La publicación de la UE, www.edps.europa.eu, dice con relación a los datos personales:

> "cualquier información sobre una persona física puede ser considerada "dato personal" si la persona está identificada o es identificable. La persona puede estar identificada directamente por su nombre, o ser identificable a través de un identificador (por ejemplo, un número de referencia) o de una combinación de elementos específicos característicos de su identidad (por ejemplo, su edad, nacionalidad y función). Son datos personales, por ejemplo, el nombre y los apellidos, la fecha de nacimiento, las fotografías, las direcciones de correo electrónico, los números de teléfono y los números personales. También se consideran datos personales los relativos a la salud del interesado, los datos empleados para fines de evaluación o los datos de tráfico sobre el uso de Internet".

Cabe decir que el Convenio 108, de 28 de enero de 1981, define el dato personal como toda información concerniente a una persona física identificada o identificable.

La web oficial de la Unión Europea[24] con fecha de 31/01/2021, mantiene una página que contestan a varias preguntas sobre el RGPD y en concreto contesta a la pregunta ¿qué son los datos personales? a lo cual dice literalmente:

> "Los datos personales son cualquier información relacionada con una persona identificada o identificable, también denominada "el interesado". Ejemplos de datos personales:
>
> - nombre y apellidos
> - dirección
> - número de documento de identidad/pasaporte
> - ingresos
> - perfil cultural
> - dirección de protocolo internet (IP)
> - datos en poder de hospitales o médicos (que identifican únicamente a una persona con fines sanitarios)."

Finalmente, la Agencia Española de Protección de Datos público en octubre del año 2019 en la "Protección de Datos: Guía para el ciudadano", primera edición fue en diciembre de 2016, en el cual define lo que entiende por dato personal, diciendo:

> "los datos de carácter personal son cualquier información referente a personas físicas identificadas o identificables, pudiendo ser identificable toda persona cuya identidad pueda determinarse mediante un identificador (por ejemplo, un nombre, un número de identificación, datos de localización o un identificador en línea) o mediante el uso de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de las personas".

La AEPD utiliza el artículo 4.1 del RGPD para definir el concepto de dato de carácter personal tal como deja constancia en la Resolución del procedimiento sancionador de 11 de junio de 2019[25]. La AEPD entiende que la identificabilidad de una persona a través de un dato define el dato como dato personal[26].

[24] YOUR EUROPE. "Reglamento general de protección de datos. ¿Cuándo se aplica el Reglamento general de protección de datos (RGPD)?" Web oficial de la UE. Disponible en https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm (28/02/2021).

[25] AEPD (2019) Resolución de la Agencia Española de Protección de Datos PS/00236/2018, de 11 de junio de 2019. FF 5. p 44/85.

[26] AEPD (2019) Informe del Gabinete Jurídico sobre el Interés Legítimo. Septiembre de 2019. Disponible en https://www.aepd.es/ sites/default/files/2019-09/informe-juridico-rgpd-interes-legitimo.pdf (28/02/2021). (28/02/2021). p 2.

Nota crítica: El texto legal del Reglamento (UE) define a la expresión dato personal y los confunde con la expresión información personal, que como ya se ha analizado, dato e información no son sinónimos[27].

En el artículo 4 del Reglamento (UE) 2016/679 se define dato personal como toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

1.4. Dato y dato en informática

No es infrecuente encontrar expresiones que vinculan de una forma íntima y casi exclusiva los conceptos de datos con la informática, lo digital e internet. De esta forma es aconsejable detenerse en cada uno de ellos y precisar su significado y alcance.

Es evidente que, si bien el dato, recientemente en la historia de la sociedad, está indisolublemente unido con la informática, no todos los datos tienen soporte informático, pues es sabido por todos que, desde que el hombre registra sus actos, hay otros soportes en donde se almacenan datos existiendo distintos medios de transmisión de los mismos.

De igual forma que los documentos, definidos en la Norma ISO 9000:2005, los datos pueden presentarse por escrito, en imagen, en vídeo, en audio o de otra cualquier otra manera. Ejemplo de ello es el ritmo del latido cardiaco, un dato que el médico utilizará para conformarse una información acerca del estado de salud de su paciente. Este dato puede ser descrito por el facultativo en base a la directriz del conocimiento clínico o también pueden ser almacenadas en archivos de sonido o traducido por un equipo de electromedicina a una tira de papel, el electrocardiograma. El Considerando 15 del Reglamento (UE) 2016/679 dice al respecto "A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas".

En apartados anteriores ya se ha intentado delimitar el significado del concepto dato y documento. En cuanto a la informática o computación, se entiende como aquel proceso mediante el cual se trata automáticamente datos a través de dispositivos tecnológicos, electrónica y sistemas computacionales.

> "De manera general, podemos definir la informática como cualquier actividad orientada a objetivos que requiera, se beneficie o cree computadoras. Por lo tanto, la informática incluye el diseño y la creación de sistemas de hardware y software para una amplia gama de propósitos: procesamiento, estructuración y administración; diversos tipos de información; hacer estudios científicos utilizando computadoras; hacer que los sistemas informáticos se comporten de manera inteligente; crear y utilizar medios de comunicación

[27] *Vid. Infra p 23,* capítulo 1.1., del Título I.

> y entretenimiento; buscar y recopilar información relevante para cualquier propósito en particular, etc. La lista es prácticamente infinita y las posibilidades son vastas"[28].

La informática o un sistema informático permite almacenar y procesar datos o información, mediante la interacción del hardware o cualquier tipo de dispositivo físico de carácter tecnológico, del software y de personal especializado.

El almacenamiento en informática no significa que todo lo que se almacena pude luego tratarse de igual forma. No todo soporte digital o electrónico permite un tratamiento automatizado de lo que incluye o hay en el soporte. Una cosa es la gestión de documentos en soporte informático y la otra es a la gestión de bases de datos relacionales. Es evidente que se puede introducir un documento en un soporte digital haciendo fotos de las páginas o bien se puede introducir el documento en un procesador de texto y gráficos que nos permitirá tratar todos los datos de forma independiente e individualizada. De esta forma se debe distinguir en la tecnología de la información la gestión de documentos en su modalidad gestión documental o de gestión informática en su modalidad de gestión de base de datos de forma relacionada o gestión de bases datos relacionales[29]. Un sistema nos permitirá el tratamiento de dato automatizadamente y el otro sistema tratará el documento como un dato, pero no permitirá tratar lo que podrían ser datos internos del documento como datos aislados.

El Software incluye el sistema operativo o conjunto de programas que gestionan los dispositivos del hardware, el firmware o soporte lógico inalterable y aplicaciones o programas informáticos o software de aplicación dirigidos a que el usuario pueda realizar diversas tareas o funcionalidades, siendo importantes los sistemas de gestión de bases de datos los cuales son los que permiten la entrada o captación de los datos, el procesamiento de los mismos y la salida o transmisión de los resultados, y el conjunto de estas tres tareas se conoce como algoritmo.

Los datos de las redes y sistemas de información tienen su propia norma de protección. Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones son todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales; los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos, disponen de su propia normativa en cuanto a su seguridad. El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, es el que regula la seguridad de las redes y sistemas de información.

[28] IEEE COMPUTER SOCIETY (2005) "Computing Curricula 2005: The Overview Report" The Joint Task Force for Computing Curricula 2005. USA. ACM and IEEE. p 9.

[29] CORTINA LL. (2015) "Sistemas de Gestión de Bases de Datos Documentales Características Principales y Metodología de diseño". Barcelona. Universitat Pompeu Fabra. pp 11-12.

Esta confusión no es tan solo teórica. En la Comunidad de Madrid implica y arrastra todo el desarrollo normativo que necesita la propia normativa de protección de datos, pues difícilmente se podrá conciliar esta acción administrativa con las figuras, obligaciones y responsabilidades del responsable y del encargado del tratamiento en los centros sanitarios públicos, tal como veremos en el TITULO III[30].

El Comité de Seguridad de la Información de la CSM, en virtud de las competencias de la Orden 491/2013 de 27 de junio de la Consejería de Sanidad, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica, da soporte a la creación de una figura colegiada que suple al delegado de protección de datos en la Consejería de Sanidad en la Comunidad de Madrid desde el mes de abril de 2018. La Viceconsejería de Sanidad de la Comunidad de Madrid comunica el día 27 de abril de 2018 a la Agencia Española de Protección de Datos la creación de una figura colegiada denominada Comité Delegado de Protección de Datos. Esta figura colegiada, atípica, no consta en el Reglamento 2016/679 ni la Ley Orgánica 3/2018, pero no tan solo sorprende por atípica y por no estar amparada por ni la Ley Orgánica 3/2018 ni por el Reglamento 2016/679 sino que obvia y omite, al parecer, que el Reglamento 2016/679 y la Ley Orgánica 3/2018 no excluyen, ni muchos menos, a los datos y a la información que están soportados en documentos de papel, gráficos, en imágenes y en sonidos y que nada tienen que ver con los sistemas informáticos. El artículo 2.1 del Reglamento 2016/679 dice: "se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero." Con esta justificación la Viceconsejería parece que reinterpreta el Reglamento 2016/679, posicionándolo tan solo como legislación relativa al tratamiento de datos informáticos.

1.5. Documento, fichero, registro y soporte documental. La gestión documental

Cualquier documento es habitualmente el soporte del resultado del tratamiento, proceso o de la utilización de los determinados datos, es decir, sin datos no hay documento.

La creciente heterogeneidad de los documentos producidos por las Administraciones públicas y por los particulares, los cambios derivados de la incorporación de las tecnologías de la información y de la comunicación, la aparición de nuevos modelos de gestión, con sistemas mixtos digitales y en papel, y el reconocimiento de una serie de derechos ciudadanos que inciden en la gestión documental y archivística, han configurado un nuevo escenario que demanda completar el tratamiento tradicional de los archivos con una regulación de mayor alcance y perspectiva, así se desprende del Real Decreto 1708/2011, de 18 de noviembre.

Al referirnos a los documentos en busca de una definición genérica y al mismo tiempo ampliamente aceptada nos debemos dirigir al estudio de las normas ISO y concretamente ISO 9000:2005, que es la norma sobre "sistemas de gestión de la

[30] *Vid*. *Infra p 417*, capítulo 6.3 del TITULO III

calidad" que ha definido los documentos y registros. España participa en la ISO a través de La Asociación Española de Normalización (UNE).

La Asociación Española de Normalización y Certificación se constituye en el año 1986, cuyo embrión se ubica en 1935 como Asociación Española de Normalización, al amparo de la Ley de Asociaciones 191/1964, siendo ese mismo año designada por el entonces Ministerio de Industria y Energía como entidad reconocida para desarrollar tareas de normalización[31]. En el año 2017, 1 de enero de 2017, se concreta como entidad privada, multisectorial y sin fines lucrativos, designada por el Ministerio de Economía, Industria y Competitividad como organismo nacional de normalización. Las normas de referencia son la Ley 21/1992, de 16 de julio, de Industria, y el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y la seguridad industrial.

Según la norma ISO 9000:2005, un documento se define como la información (datos significativos) y su medio de soporte. Un documento puede estar escrito, estar en vídeo, en una muestra física, en plano, en un programa de ordenador, en un audio o en otra cualquier otra manera que permita evidenciarlo.

Etimológicamente documento proviene de *docere* al igual que docencia. Según la Real Academia Española documento viene de *documentum* y significa "diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos." También se le conoce como "escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo". Por otra parte, la RAE también lo define como "cosa que sirve para testimoniar un hecho o informar de él, especialmente del pasado. Un resto de vasija puede ser un documento arqueológico." Por último, también es "una instrucción que se da a alguien como aviso y consejo en cualquier materia."

Tradicionalmente, documento hacia y hace referencia a un texto en soporte papel escrito a mano o mediante algún instrumento mecánico, que se graba o marca mediante algún tipo de tinta o colorante con intención de que permanezca en el tiempo, con criterio de durabilidad. A lo cual se añade la posibilidad de que describan situaciones, narrativas, sentimientos, voluntades, ideas y datos. Desde mediados del siglo XX se introdujo otro tipo de documentos, estos son los que hacen referencia al entorno informático, también conocidos por ficheros.

El concepto de fichero viene referido al conjunto de fichas ordenadas. La Real Academia Española define fichero como conjunto de fichas ordenadas, a lo cual aplica un ejemplo, "consultar el fichero de una biblioteca; aparecerán en este fichero, ordenados según sus apellidos, los traductores, prologuistas e ilustradores"; pero también se refiere a fichero como "mueble o caja que sirve para guardar fichas de manera ordenada". A su vez, ficha se entiende a criterio de la RAE como "pedazo de papel, plástico u otro material donde

[31] UNE (2020) "Nuestra Historia ". Asociación Española de Normalización. Disponible en https://www.une.org/la-asociacion/historia (31/05/2020).

se consignan datos, normalmente identificativos o informativos de una cosa o persona, para catalogarlo, clasificarlo o archivarlo junto con otros del mismo tipo".

El Reglamento (UE) 2016/679, en su artículo 4 define en su apartado 6) fichero como: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica. Cuestión fundamental, dado que el artículo 2.1 sobre el ámbito material del Reglamento entiende que el presente Reglamento se aplica al "tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

El Reglamento (UE) 2016/679, plantea una seria duda sobre el ámbito de aplicación de la norma, dado que no aclara el soporte del dato, tan solo en el artículo 2 se refiere a "datos personales contenidos o destinados a ser incluidos en un fichero". Es decir, admite cualquier soporte.

El Reglamento (UE) se refiere a que el ámbito material de la norma es el tratamiento de los datos, ya sea este tratamiento automatizado o manual, siempre y cuando el dato vaya a ser incluido en un fichero. Sin embargo, no aclara a qué tipo de fichero se refiere, si al fichero entendido con carácter general (conjunto de fichas ordenadas; siendo fichas todo pedazo de papel, plástico u otro material donde se consignan datos) o bien se refiere a fichero como un conjunto de registros informáticos o automatizados.

Para concretar el concepto de fichero en el marco del RGPD cabe acudir a la Sentencia del Tribunal de Justicia de 10 de junio de 2018. Esta sentencia en su Fallo 2 entiende que el concepto fichero, en el marco de la petición prejudicial planteada, comprende un conjunto de datos personales recogidos manualmente en relación con una actividad concreta y predeterminada, consistentes en nombres, direcciones y otra información relativa a las personas contactadas, estando estos datos estructurados según criterios determinados que permitan, en la práctica, recuperarlos fácilmente para su utilización posterior. La sentencia añade, que para que dicho conjunto de datos esté comprendido en ese concepto de fichero no es preciso que incluya fichas, catálogos específicos u otros sistemas de búsqueda[32].

El anexo del ENI (Esquema Nacional de Interoperabilidad) RD 4/2010, de 8 de enero, define el documento electrónico como: "información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado, y susceptible de identificación y tratamiento diferenciado"[33].

Por documento en informática o documento digital debe entenderse como aquel documento que utiliza los inputs electrónicos del lenguaje magnético, a través de

[32] STJUE de 10 de julio de 2018 (Gran Sala) (Asunto C-25/17), F 2.

[33] ENI (2016). Portal de Administración electrónica. Gobierno de España. Documento electrónico. Guía de aplicación de la Norma Técnica de Interoperabilidad 2ª edición electrónica. Dirección de Tecnologías de la Información y las Comunicaciones (DTIC). Ministerio de Hacienda y Administraciones Públicas. 2ª edición de Julio de 2016. Disponible en https://administracionelectronica.gob.es/pae_Home/ pae_Estrategias/ pae_Interoperabilidad_Inicio/ pae_Normas_tecnicas_de_interoperabilidad.html (28/02/2021).

tecnología digital, para ser grabado y que constituye la acreditación y materialización de su voluntad pudiendo contener representaciones de texto, imagen, sonido, animación o video. Los documentos electrónicos tienen las características de inalterabilidad, seguridad, durabilidad y autenticidad.

El documento electrónico se escribe en lenguaje binario o diádico, en un determinado lenguaje o código, consta de un soporte material bien sea disco, cintas, redes, chips o circuitos y puede ser atribuido a una persona en calidad de autor a través de una forma digital, clave o llave electrónica. Es un sistema de numeración en el que los números se representan utilizando solamente las cifras 0 y 1[34].

El Real Decreto 1708/2011, de 18 de noviembre define como documento electrónico de acuerdo con lo establecido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, "la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado."

Según el artículo 26.1 de la Ley 39/2015[35] se entiende por documentos públicos administrativos "los válidamente emitidos por los órganos de las Administraciones Públicas. Las Administraciones Públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia."

El documento, tenga el soporte que tenga, es una de las bases del derecho y puede entenderse como el soporte de la constancia fehaciente de algo, de una cosa material o inmaterial. En el ordenamiento jurídico español es el Código Civil (C.c.) el que clasifica los documentos de públicos y privados. Los documentos privados no son definidos, pero si regulados en los artículos 1225 a 1230 del C.c. Los documentos públicos son definidos en el artículo 121 del Código Civil. La Ley de Enjuiciamiento Civil define al documento privado por exclusión en su artículo 324.

Dejando al margen las leyes más al uso, como el Código Civil o la Ley de Enjuiciamiento Civil, el ordenamiento jurídico español entiende que documento es:

1. todo soporte material que exprese o incorpore datos, hechos o narraciones (artículo 26 del Código Penal).
2. (artículo 48 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común) es:

> "cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad,

[34] MANDADO PÉREZ, E., MANDADO RODRÍGUEZ, Y. (2015) "Sistemas electrónicos digitales". Marcombo ediciones técnicas. 10ª Edición. pp 8-9.

[35] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por esta u otras Leyes."

3. es toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material incluso los informáticos (artículo 28 de la Ley de Patrimonio Histórico Nacional)
4. acepta el valor probatorio en juicio del soporto electrónico en el que conste un contrato celebrado vía electrónica (El artículo 24.2 de Servicios en la sociedad de la información, ley 34/2002)
5. define los documentos electrónicos y distingue los documentos electrónicos públicos de los privados (artículo 3 de la ley de firma electrónica, ley 59/2003)
6. documento electrónico es "información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado, y susceptible de identificación y tratamiento diferenciado". (anexo del ENI RD 4/2010, de 8 de enero)

Todo ello en conjunto permite ver la íntima y neta relación entre dato y documento, pues el documento es todo aquel soporte que exprese datos.

Por último, la gestión documental desde el punto de vista informático significa la gestión de documentos almacenados en un soporte electrónico o digital, trata a cada documento como tal, como un solo dato, no suele tratar a los datos internos del documento. Ejemplo de ello son los PACS, sistema de almacenamiento y distribución de imagen, "corresponde a la traducción literal de sus siglas Picture Archiving and Comunications System. Normalmente asociamos este sistema a Radiología, debido a que este servicio es el principal generador de imagen de un hospital y además el de mayor consumo."[36]

1.6. Tipos y subtipos de datos en el Reglamento 2016/679 y Ley Orgánica 3/2018

Unas de las primeras preguntas que surgen de la lectura del Reglamento 2016/679 y de la Ley Orgánica 3/2018, es ¿a qué tipo de datos afecta? El Reglamento 206/679 define el ámbito de aplicación material en su artículo 2.1 "El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."

La primera pregunta que surge sobre este artículo es conocer el significado que le da el Reglamento (UE) al término automatizado. De forma intuitiva, lo habitual es asimilar automatizado con informático y digital, ambos electrónicos, pero, a su vez, distintos, según lo visto en el apartado anterior. No todo soporte digital o electrónico permite un tratamiento automatizado de lo que incluye el soporte. Tal como ya hemos visto una cosa es la gestión de documentos en soporte informático y la otra es a la gestión de bases de datos relacionales.

[36] BORDILLS I ROVIRA, F. CHAVANIA DIAZ, M. (2004), "Almacenamiento y transmisión de imágenes. PACS" Monográfico: Radiología Digital. Revista de la sociedad Española de Informática de la Salud, 45, 54-58. p 54.

Por ejemplo, achicar en un soporte informático una foto que contenga datos de la analítica de un paciente no es lo mismo que introducir dichos datos en un base de datos que permita su tratamiento. Por ejemplo, el almacenamiento digital o electrónico de una historia clínica podría realizarse bien, mediante imágenes de las páginas de los documentos a modo de gestión documental lo cual solo permitiría manejar la página archivada como una imagen, pero no permitiría directamente o automáticamente tratar su contenido o bien, mediante la introducción los datos del paciente en un formato de base de datos que dan, a su vez, contenido a los informes predeterminados de la historia clínica.

Cuando el artículo del RGPD se refiere a "tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero", evidentemente se refiere a datos en papel, sin embargo, la condición "destinados a ser incluidos en un fichero" nos puede llevar a deducir que fichero es sinónimo de informático o automatizado, y sin embargo como veremos en al apartado 7 de este mismo capítulo, no parece ser sinónimo uno de otro.

Si este artículo del RGPD lo aplicamos por ejemplo a un hospital, es evidente que es de aplicación a la historia clínica del paciente. Sin embargo, cuando la interpretación es restrictiva surgen una serie de preguntas en base al soporte de dicha historia clínica, estas son, ¿el RGPD afecta a los datos de la historia clínica en soporte papel o afecta sólo a los datos de la historia clínica en soporte informático, electrónico o digital? ¿cómo debe interpretarse "datos de la historia clínica en papel cuando estos vayan a ser incluidos en la historia clínica electrónica o digital"?, ¿cuándo se refiere al dato en papel, debe tenerse en consideración sólo cuando este acabará siendo utilizado como un dato en soporte informático?

Por lo comentado en los aportados 4 y 5 de este mismo capítulo y en base al Considerando 15 "la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas", se entiende que el RGPD incluye tanto al dato en soporte papel como al dato en suporte informático.

Por otra parte, el artículo 2.1 del Reglamento (UE) 2016/679 al decir "El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero." No dice nada de los datos biométricos, pues este tipo de datos no tienen que ser necesariamente automatizados ni automatizables en un futuro, pues la imagen por una cámara de video puede permitir identificar a una persona sin utilizar sistema automatizado ni sistema informático ninguno.

Los datos biométricos están incluidos sin ningún género de dudas en el Reglamento (UE) 2016/679, dado que son parte de las categorías especiales de datos personales incluidas en el artículo 9 Reglamento (UE) 2016/679 al decir "1. Quedan prohibidos ……, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, ……" A lo cual el Considerando 51 matiza, en cuanto al dato biométrico

> "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas

> en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física."

Sin embargo frente a este Considerando 51 se sitúa el artículo 4.14) del Reglamento (UE) 2016/679 14) que define a los datos biométricos como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

En este orden de cosas, los datos relativos a la salud en muchos casos no precisas de ser automatizados. Un ejemplo práctico es la temperatura corporal de una persona, el dato es un dato de salud y atañe a una persona. En este sentido el 30 de abril de 2020 se ha pronunciado la AEPD, en el Comunicado de la AEPD (Anexo[B]), incluyendo el dato de la temperatura de la toma de temperatura de una persona como protegido por el RGPD, sin especificar el soporte, al decir

> "Este tratamiento de toma de temperatura supone una injerencia particularmente intensa en los derechos de los afectados. Por una parte, porque afecta a datos relativos a la salud de las personas, no sólo porque el valor de la temperatura corporal es un dato de salud en sí mismo sino también porque, a partir de él, se asume que una persona padece o no una concreta enfermedad, como es en estos casos la infección por coronavirus."

Además, tal como afirma la AEPD en el comunicado del día 30 de abril 2020, en algunos casos el dato biométrico como es el de una cámara sensible a los rayos infrarrojos además aportada datos sobre la salud de la persona en el momento de la toma y datos sobre la salud de la persona fuera del espacio temporal de la toma, al decir

> "Sin embargo, dependiendo del tipo de tecnología que se emplee, puede ser necesario tomar en consideración otros elementos que, aunque relacionados con los mencionados, tienen una especial incidencia en una u otra de esas diferentes tecnologías.
>
> Este es el caso de las cámaras térmicas, a las que ya se ha hecho alusión, en la medida en que pueden ofrecer posibilidades adicionales a la toma de temperatura y que, por ello, deben ser utilizadas prestando especial atención a los principios de limitación de finalidad y minimización de datos establecidos por el artículo 5.1 RGPD."

Una lectura detenida nos permite analizar los distintos tipos de datos que tratan las normas que regulan el tratamiento de los datos más allá las distinciones expresas o calificativos propios que aparecen en sus textos.

Los textos se refieren a todos los datos, con carácter general, y califican a varios tipos de ellos. Uno de estos son los datos de "categorías especiales" (artículo 9 del Reglamento 2016/679 y articulo 9 de la Ley 3/2018), tratado en el siguiente punto. Otros son los datos personales relativos a condenas e infracciones penales (artículo 10 del Reglamento 2016/679 y articulo 10 de la Ley 3/2018) y otros son los datos sin identificación personal (artículo 11 del Reglamento 2016/679). Sin embargo, para estos textos legales, sin duda, hay más tipos de datos.

El texto a medida que define cada uno de los aspectos que incluye en su articulado va utilizando el término dato y fruto de este hecho va definiendo en cada caso lo que entiende por ello.

En este orden de cosas, en la tabla del Anexo[C] aparece un listado con treinta (30) expresiones que califican a los datos en ambas normas. En el análisis de estos treinta tipos de datos que consta en el Anexo [C] se añade en cada caso el texto legal en el cual aparece.

El listado de tipos o subtipos de datos en base al criterio empírico dado por la utilización del concepto tanto en el Reglamento (UE) 2016/679 y la Ley Orgánica 8/2018 y que consta en el Anexo [C], es el que sigue a continuación como datos: anonimizados, biométricos, bloqueados, de carácter personal, censales, clínico-asistenciales, concretos, de contacto, exactos, facilitados, con fines de interés público, genéticos, de identificación, de identificación personal del paciente, así como, datos personales procedentes de las imágenes y sonidos, imprescindibles para identificar, incompletos, inexactos, de localización, necesarios, a lo cual añade, dato o documento obtenido, personal, dato personal rectificado, dato de menores de edad, dato de salud (dato en el ámbito de la salud), dato en la investigación de la salud, dato seudonimizado, dato de tráfico, dato tributario y dato relativo a la vida sexual.

1.7. Categorías especiales de datos

En el punto anterior se han visto los distintos tipos y subtipos de datos que afloran de la normativa vigente de protección de datos de personas. Estos tipos y subtipos de datos en muchas ocasiones no vienen explícitamente diferenciados pero el contenido y el texto de la propia norma califican a unos y a otros. Los datos de las categorías especiales de datos son tratados por la norma expresamente de formar distinta que el resto de datos configurándoles una protección especial en su tratamiento.

Las normas relativas a la protección de datos que rigen en el ordenamiento jurídico español al referirse a datos especialmente protegidos o a categorías especiales de datos hacen referencia a los datos relativos a la ideología, religión, creencias, origen racial, salud, vida sexual, etnia y afiliación sindical. También se incluyen en este tipo de datos los datos de carácter personal relativos a infracciones penales o administrativas, aunque el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 han derivado este dato a otro artículo distinto de tal forma que ya no lo consideran incluido dentro de la lista de los datos con categorías especiales.

Este epígrafe 7 del capítulo 1 del Título I, se aborda analizando conjuntamente el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 con las normas que les han precedido en cada uno de sus ordenamientos jurídicos, estas son: la Ley Orgánica 5/1992, de 29 de octubre; la Ley Orgánica 15/1999, de 13 de diciembre; y la Ley Orgánica 3/2018, de 5 de diciembre. Por otra parte, se hace mención a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

En el epígrafe 1.7.5 de este mismo capítulo 1 del Título I se adjunta un cuadro comparativo de las denominaciones que en cada caso se han dado a las categorías especiales de datos.

1.7.1. El antecedente de la Ley Orgánica 5/1992, de 29 de octubre

En el Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, fue pionera en la catalogación de este tipo especial de datos, apareciendo en su exposición de motivos la expresión "datos sensibles", a tenor literal: "los denominados "datos sensibles", como pueden ser, de una parte, la ideología o creencias religiosas -cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2- y, de otra parte, la raza, la salud y la vida sexual."

Esta primera ley de protección de datos no habla de categorías especiales de datos, sino de datos especialmente protegidos, en su artículo 7 y entre los cuales incluye la ideología, religión y creencias, apelando al artículo 16.2 de la Constitución española de 1978, necesitando su tratamiento siempre del consentimiento de la persona titular de los datos.

El tratamiento de estos datos especialmente protegidos requiere el consentimiento del interesado junto al derecho de no prestarlo.

A estos tres tipos de datos especialmente protegidos se suman los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual y añade que su protección vendrá dada porque sólo podrán ser recabados, tratados automatizadamente y cedidos cuando el afectado consienta expresamente, pero también cuando por razones de interés general cuando así lo disponga una Ley.

El tratamiento de estos datos especialmente protegidos podrá se permitido además de por el consentimiento del interesado, cuando por razones de interés general lo disponga una ley. Los datos mencionados, excepto los de salud, quedan protegidos por la prohibición de ser almacenados en ficheros cuya finalidad sea el almacenamiento.

En cuanto a los datos de carácter personal relativos a infracciones penales o administrativas, la Ley limita su tratamiento en los supuestos previstos en la ley.

1.7.2. El antecedente de la Ley Orgánica 15/1999, de 13 de diciembre

La Ley que sucede a la anterior, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sigue con la misma expresión y vuelve a referirse a los datos especialmente protegidos y también lo hace en su artículo 7. Esta ley 15/1999 mantiene la redacción de la anterior sin muchas variaciones, vuelve a apelar al artículo 16.2 de la Constitución española de 1978 en relación con la ideología, religión o creencias y mantiene las dos exigencias para el tratamiento de estos datos, por una parte, el consentimiento del afectado y, por otra parte, el interés general declarado por una ley.

Las novedades de esta ley 15/1999 son tres: introduce dos nuevos tipos de datos, el dato de la afiliación sindical y el dato étnico; e introduce tres excepciones a la obligación de consentimiento del afectado.

El dato de afiliación sindical se ubica dentro de los que requieren siempre consentimiento del afectado. En su punto cuatro añade los datos étnicos junto a los raciales. La RAE a fecha de abril de 2020 define por etnia: "comunidad humana definida por afinidades raciales, lingüísticas, culturales, etc." y étnico: "perteneciente o relativo a una nación, raza o etnia". La RAE a fecha de abril de 2020 define por raza: "cada uno de los grupos en que se subdividen algunas especies biológicas y cuyos caracteres diferenciales se perpetúan por herencia; o casta o calidad del origen o linaje".

Por otra parte, la ley introduce tres excepciones al consentimiento del afectado. La primera excepción, afecta a los datos relativos a ideología, afiliación sindical, religión y creencias, y exceptúa a los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del interesado.

La segunda excepción, afecta a los datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual, y exceptúa la necesidad de consentimiento cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios. Esta excepción tiene una condición, esta es que: "siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto."

La tercera y última excepción, afecta a los datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento o el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona. Mantiene la prohibición de crear ficheros de almacenamiento para los datos a la ideología, religión, creencias, origen racial y vida sexual, y añade esta prohibición a los datos de etnia y de afiliación sindical.

En cuanto a los datos de carácter personal relativos a infracciones penales o administrativas, no hay variación con relación a la anterior Ley Orgánica.

1.7.3. La Ley Orgánica 3/2018, de 5 de diciembre

Es en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en donde aparece por primera vez, la expresión categorías especiales de datos, en el artículo 9. Este artículo hace tan solo una referencia al artículo 9 (Tratamiento de categorías especiales de datos personales) del Reglamento 2016/679, sin introducir novedad normativa ninguna.

La Ley Orgánica 3/2018 está atada al Reglamento 2016/679, tal como establece el ordenamiento jurídico de la Unión Europea en cuanto al derecho derivado y sus efectos en los Países miembros. Este Reglamento introduce y modifica los datos personales de categoría especial que regían en el ordenamiento jurídico de la Unión Europea y de España, en consecuencia, se entiende que esta ley asume la existencia de un nuevo

listado de datos de esta categoría: opiniones políticas (ideología), convicciones religiosas (religión), convicciones filosóficas (creencias), de afiliación sindical, origen racial, origen étnico, salud, orientación sexual, salud, genéticos y biométricos. Retirando de esta categoría a los datos de naturaleza penal que los remite al artículo 10 (Tratamiento de datos personales relativos a condenas e infracciones penales)

En relación con la anterior Ley Orgánica 15/1999, la actual Ley Orgánica 3/2018 modifica:

a) Sustituye la expresión vida sexual por orientación sexual. Mientras el Reglamento 2016/679 mantiene las dos expresiones.
b) Suprime la referencia explícita a la salud del listado de datos de categoría especial. Refiriéndose implícitamente al dato de salud a través del artículo 9.2 que remite la Ley Orgánica a lo dispuesto en el artículo 9.2. del Reglamento (UE) 2016/679 en sus puntos g), h) e i).
c) Retira del listado a los datos de carácter personal relativos a la comisión de infracciones penales o administrativas y los remite al artículo 10 (Tratamiento de datos de naturaleza penal). Ocurre lo mismo en el Reglamento 2016/679, ubica los datos de naturaleza penal en el artículo 10 (Tratamiento de datos personales relativos a condenas e infracciones penales)
d) Introduce una nueva limitación al consentimiento del afectado, esta es, siempre que no vaya en contra del Derecho de la Unión o de los Estados miembros al prohibir levantar la prohibición del artículo 9.1 por parte del interesado mediante su consentimiento. Esta limitación no existente en la Ley Orgánica 15/1999, pero que aparece en el artículo 9 del Reglamento 2016/1999. Pero a su vez, vuelve a regular dicha limitación al decir que ello no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.
e) Introduce una reserva de ley, en el artículo 9.2. en sus letras g), h) e i), que son las que hace referencia el Reglamento (UE) 2016/679 a las condiciones que se pueden dar para no exigir el consentimiento en el tratamiento de los datos de salud.

Para entender correctamente el artículo 9 (Categorías especiales de datos) de la Ley Orgánica 3/2018 es absolutamente imprescindible estudiar y entender el artículo 9 (Tratamiento de categorías especiales de datos personales) del RGPD.

1.7.4. El Reglamento (UE) 2016/679

El Reglamento (UE) 2016/679 es la norma de la Unión Europea sobre protección de datos personales. La norma anterior al Reglamento (UE) 2016/679 del Parlamento 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, es la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Esta Directiva fue la primera norma en utilizar la expresión "categorías especiales de datos" al referirse a su tratamiento en el artículo 8 (Tratamiento de categorías especiales de datos). Este artículo prohíbe el tratamiento de los datos personales que incluye en su listado, estos son: opiniones políticas, convicciones religiosas, convicciones filosóficas (creencias), de pertenencia a sindicatos, salud y sexualidad.

Así pues, el artículo 9 del Reglamento (UE) 2016/679 (Tratamiento de categorías especiales de datos personales) prohíbe el tratamiento de datos personales cuando estos datos se incluyan dentro del siguiente listado: origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, la afiliación sindical, datos genéticos, datos biométricos, datos de la salud, datos relativos a la vida sexual o las orientaciones sexuales de una persona física. Este listado amplía considerablemente el que disponía la Directiva La Directiva 95/46/CE del Parlamento Europeo y del Consejo, concretamente se amplía en las siguientes categorías:

- datos de la raza
- datos étnicos
- datos genéticos
- datos biométricos

La prohibición realizada por el Reglamento (UE) 2016/679 viene a reforzar la no autorización genérica que hace el reglamento sobre el tratamiento de cualquier dato personal. De esta manera, de forma similar a la Directiva 95/46/UE, la nueva legislación además de no legitimar cualquier tratamiento sino solo los del *numerus clausus* del artículo 6 además prohíbe el tratamiento de determinados datos, tal como aparece en el artículo 9 (Tratamiento de categorías especiales de datos personales) del Reglamento 2016/679 y que de forma referida hace mención el artículo 9 (Categorías especiales de datos) de la Ley Orgánica 3/2018.

A todo lo cual hay que añadir la cláusula de legitimación de terceras personas se encuentra en el punto 3 del artículo 9 del Reglamento 2016/679, en este orden literal:

> "3.Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes."

En conclusión, la legitimación de terceras personas se establece en base a la base jurídica de la obligación de secreto profesional, lo cual será analizado en el capítulo 5.5 del Título I.

1.7.5. Listado de los datos de categoría especial, en cada norma. Análisis comparativo

En este apartado, la investigación se detiene en revisar uno a uno todos los datos que el Derecho de la Unión y la legislación española incluyen explícitamente dentro de lo que viene a entenderse por categorías especiales de datos.

La tabla (Tabla 1) ubicada en esta página, presenta cinco columnas distintas y cada una de ellas recibe una denominación que representa el año en el que se publicó el texto normativo y la letra que corresponde, en la base de la tabla, al nombre concreto de la norma a la cual hace referencia la columna.

Cada columna describe todos los datos incluidos dentro de la denominación "Categoría especial de datos", en las columnas (c) a (e), o "datos de especialmente protegidos", en las columnas (a) y (b).

Tabla 1. Listado de datos de categorías especiales de 1992 a 2018 (elaboración propia)

año 1992 (a)		año 1995 (b)		año 1999 (c)		año 2016 (d)		año 2018 (e)	
1	ideología	1	opiniones políticas	1	ideología	1	opiniones políticas	1	ideología
2	religión	2	convicciones religiosas	2	religión	2	convicciones religiosas	2	religión
3	creencias	3	convicciones filosoficas	3	creencias	3	convicciones filosoficas	3	creencias
		4	pertenencia a sindicatos	4	afiliación sindical	4	afiliación sindical	4	afiliación sindical
4	origen racial			5	origen racial	5	origen racial	5	origen racial
				6	origen étnico	6	origen étnico	6	origen étnico
5	vida sexual	5	sexualidad	7	vida sexual	7	orientación sexual	7	orientación sexual
6	salud	6	salud	8	salud	8	salud	8	Salud (implicitamente)
7	penal			9	penal				
						9	genéticos		
						10	biométricos		

a	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal
b	Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
c	la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
d	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
e	Reglamento (UE) 2016/679 del Parlamento 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

Las normas que utilizan la expresión "categoría especial de datos" no lo hacen de la misma forma. Mientras que la Ley Orgánica 3/2018 denomina a su artículo "Categorías especiales de datos", el Reglamento (UE) 2016/679 utiliza la expresión "Tratamiento de categorías especiales de datos personales" y la Directiva 95/46/CE "Tratamiento de categorías especiales de datos".

El significado de ambas expresiones aparentemente es el mismo, pero en realidad no es sinónimo una expresión de la otra, dado que una cosa es referirse del tratamiento de una determinada cosa y otra muy distinta es referirse a la cosa en sí misma. Sin embargo, el artículo 9 de la Ley Orgánica 3/2018 en su punto uno y dos hace una remisión expresa y explicita y sin matices, ni otras consideraciones, al artículo 9 del Reglamento (UE) 2016/679. Así pues, si la Ley Orgánica 3/2018 utiliza la expresión "Categorías especiales de datos" y a su vez remite todo su contenido al Reglamento (UE) 2016/679 que utiliza la expresión "Tratamiento de categorías especiales de datos personales" se deduce que el legislador español ha querido decir lo mismo con estas dos expresiones, bien distintas una de la otra.

En la descripción de las categorías de datos se incluyen datos relativos a ideología u opiniones políticas, a la religión o convicciones religiosas, a creencias o convicciones filosóficas, a la afiliación o pertenencia a sindicatos, al origen racial, al origen étnico, a la vida sexual, orientación sexual o sexualidad y a la salud.

En cuanto a los datos genéticos y datos biométricos, la Ley Orgánica no los incluye en el artículo 9, si bien el Reglamento (UE) los incluye en su artículo 9. La Ley Orgánica 3/2018, incluye los datos genéticos en la Disposición Adicional Decimoséptima y en la Disposición Final Undécima.

Los datos biométricos tampoco son incluidos en el artículo 9 de Ley Orgánica 3/2018, si bien el Reglamento (UE) sí que los incluye en su artículo 9. La Ley Orgánica 3/2018, incluye los datos biométricos en la Disposición Final Undécima.

En los siguientes subapartados, se describen cada uno de los tipos de datos incluidos en esta denominación genérica titulada "categorías especiales de datos especiales".

1.7.5.1. Datos relativos a Ideología u opiniones políticas

Tratamiento por los textos legales: inicialmente en la Ley de 1992 aparece como ideología, en la Directiva de 1995 pasa a tratarse como opinión política, para volver en 1999 a utilizarse el término ideología, circunstancia que vuelve a pasar en el año 2018 después de que en el Reglamento de 2016 volviera a utilizarse opinión política.

La libertad ideológica es un derecho fundamental reconocido por la Constitución Española en su artículo 16.1 del Capítulo segundo (Derechos y libertades) del Título I (De los derechos y deberes fundamentales) y que como reconoce la propia Constitución en su artículo 53, estos vinculan a todos los poderes públicos y serán regulados solos por leyes, respetando su contenido esencial, encontrándose bajo la tutela de los tribunales ordinarios en base a los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Expresión de contenido esencial:

> "Esta expresión contenido esencial, que a simple vista puede pasar desapercibida, viene escrita en la propia Constitución lo que plantea un problema de aplicación al derecho de propiedad. La idea de contenido esencial procede de la Ley Fundamental de Bonn, en la que esta expresión, contenido esencial, solo se predica exclusivamente a las libertades públicas. Esta idea de contenido esencial trata de que el desarrollo de un derecho no destruya su contenido material convirtiéndolo en un derecho puramente formal, bien entendido que el desarrollo de un derecho hace referencia a la plasmación sintáctica, semántica, formal y material del mismo y a su efectividad mediante la acción legislativa de los Parlamentos o la acción normativa de los Gobiernos, en su caso, de tal forma que la redacción de una ley no pueda alterar el espíritu, la voluntad y el alcance de un derecho fundamental o un derecho constitucional. No se puede menos que apreciar este aspecto material del derecho pues las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquellas.
>
> Los referentes históricos de la expresión contenido esencial son el artículo 19.2 de la Constitución alemana de 1949 y el artículo 18.3 de la Constitución portuguesa de 1976, entre otros. De igual manera, el artículo 17 del Convenio Europeo de Derechos Humanos prohíbe cualquier acto que pueda llevar a la destrucción de los derechos fundamentales y la Carta de los Derechos Fundamentales de la Unión Europea (Niza 2000) determina que cualquier limitación de los derechos reconocidos en ese texto debe ser establecida por

> ley y respetar su contenido esencial. Sin embargo, nada dice la CE acerca del concepto y alcance de la expresión contenido esencial de los derechos como reconoció el Tribunal Constitucional en unas de sus sentencias. La CE no determina cuál sea el contenido esencial de los derechos y libertades, por tanto, las controversias deben ser resueltas por el propio Tribunal Constitucional."[37]

La libertad ideológica está amparada por el "artículo 9. Libertad de pensamiento, de conciencia y de religión" del Convenio para la protección de los derechos humanos y de las libertades fundamentales. La Unión Europea incorporó el mandato de la adhesión al Convenio, en el apartado 2 del artículo 6 del Tratado de la Unión Europea (en los términos establecidos por su Protocolo Nº.8) en su versión consolidada tras las modificaciones introducidas por el Tratado de Lisboa, firmado el 13 de diciembre de 2007.

En consecuencia, la normativa que protege estos datos lo hace no tan solo ante el bien jurídico del derecho fundamental de la libertad ideológica el cual debe ser protegido por todo el abanico legislativo del ordenamiento jurídico, sino también para la protección de datos personales, sobre su tratamiento, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados, sino como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso (extraído de las sentencias: Sentencia del Tribunal Constitucional 94/1998, de 4 de mayo, y Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre)[38].

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado. El consentimiento del afectado no es tratado como un valor absoluto. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende consentir o autorizar su tratamiento.

1.7.5.2. Datos relativos a la religión o convicciones religiosas

Tratamiento por los textos legales: en las Leyes Orgánicas de 1992, 1999 y 2018 aparece el término *religión* y en los textos emanados del Parlamento y de la Comisión, el término utilizado es convicciones religiosas.

La libertad religiosa es un derecho fundamental reconocido por la Constitución Española en su artículo 16.1 del Capítulo segundo (Derechos y libertades) del Título I (De los derechos y deberes fundamentales) y que como reconoce la propia Constitución en su artículo 53 estos vinculan a todos los poderes públicos y serán regulados solos por leyes,

[37] BESTARD PERELLÓ, JJ. (2016) "De lo público a lo privado y viceversa". Madrid, www.amazon.es. pp 136-137.
[38] STC 94/1998 de 4 de mayo (Sala Segunda) FJ 6º y STC 292/2000 de 30 de noviembre (El Pleno) CG.

respetando su contenido esencial, encontrándose bajo la tutela de los tribunales ordinarios en base a los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional.

La libertad religiosa o de convicciones religiosas está amparada por el "artículo 9. Libertad de pensamiento, de conciencia y de religión" del Convenio para la protección de los derechos humanos y de las libertades fundamentales. La Unión Europea incorporó el mandato de la adhesión al Convenio, en el apartado 2 del artículo 6 del Tratado de la Unión Europea (en los términos establecidos por su Protocolo Nº. 8) en su versión consolidada tras las modificaciones introducidas por el Tratado de Lisboa, firmado el 13 de diciembre de 2007.

En consecuencia, la normativa que protege estos datos lo hace no tan solo ante el bien jurídico del derecho fundamental de la libertad religiosa el cual debe ser protegido por todo el abanico legislativo del ordenamiento jurídico, sino también para la protección de datos personales, sobre su tratamiento, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados, sino como un derecho autónomo e independiente tal como ya se ha descrito en el punto anterior.

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado. El consentimiento del afectado no es tratado como un valor absoluto. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende autorizar su tratamiento.

1.7.5.3. Datos relativos a creencias o convicciones filosóficas

Tratamiento por los textos legales: en las Leyes Orgánicas de 1992, 1999 y 2018 aparece el término creencias y en los textos emanados del Parlamento y de la Comisión, de los años 1995 y 2016, el término utilizado es convicciones filosóficas.

La libertad de creencias es un derecho fundamental reconocido por la Constitución Española en su artículo 16, apartados 1 y 2, del Capítulo segundo (Derechos y libertades) del Título I (De los derechos y deberes fundamentales) y que como reconoce la propia Constitución en su artículo 53 estos vinculan a todos los poderes públicos y serán regulados solos por leyes, respetando su contenido esencial, encontrándose bajo la tutela de los tribunales ordinarios en base a los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional.

La libertad de pensamiento está amparada por el "artículo 10. Libertad de pensamiento, de conciencia y de religión" del Convenio para la protección de los derechos humanos y de las libertades fundamentales. La Unión Europea incorporó el mandato de la adhesión al Convenio, en el apartado 2 del artículo 6 del Tratado de la Unión Europea (en los términos establecidos por su Protocolo Nº. 8) en su versión consolidada tras las modificaciones introducidas por el Tratado de Lisboa, firmado el 13 de diciembre de 2007.

La libertad de creencias se entiende englobada dentro del ámbito ideológico y religioso e incluso filosófico. En consecuencia, la normativa que protege estos datos lo hace no tan solo ante el bien jurídico del derecho fundamental de la libertad de pensamiento el cual debe ser protegido por todo el abanico legislativo del ordenamiento jurídico, sino también para la protección de datos personales, sobre su tratamiento, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados, sino como un derecho autónomo e independiente tal como ya se ha descrito en los dos puntos anteriores.

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado. El consentimiento del afectado no es tratado como un valor absoluto. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende autorizar su tratamiento.

1.7.5.4. Datos relativos a la afiliación o pertenencia a sindicatos

Tratamiento por los textos legales: en las Leyes Orgánicas 1999 y 2018 y en el Reglamento (UE) 2016/679 aparece el término *afiliación sindical* y en la Directiva 95/46/CE Parlamento y de la Comisión el término utilizado es *pertenencia a sindicatos*.

La libertad sindical es un derecho fundamental reconocido por la Constitución Española en su artículo 28 del Capítulo segundo (Derechos y libertades) del Título I (De los derechos y deberes fundamentales) y que, como reconoce la propia Constitución, en su artículo 53 estos vinculan a todos los poderes públicos y serán regulados solo por leyes, respetando su contenido esencial, encontrándose bajo la tutela de los tribunales ordinarios en base a los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional.

El Tribunal Constitucional se ha pronunciado en muchas ocasiones sobre la utilización de datos informáticos personales relativos a la afiliación sindical de determinados trabajadores y su relación con el derecho de libertad sindical, del artículo 18 de la Constitución española. La doctrina esgrime una serie de razones. El artículo 18 de la CE es esgrimido por el Tribunal Constitucional y determina que no tan solo es un elemento de protección de los derechos de los ciudadanos frente al uso de la informática, sino que más aun, entra de lleno en el derecho fundamental a controlar la información que concierne a cada persona. En este sentido no tan solo se protege el derecho a la intimidad, sino que se previene de la utilización de la informatización de los datos acabe en una conducta ilícita. En la concepción del TC, el art. 18.4 CE, no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, es decir, el uso de los datos personales propiciados para una determinada y concreta utilidad para otra finalidad radicalmente distinta sea esta última licita [39].

[39] MONEREO PEREZ JL., FERNÁNDEZ AVILÉS, JA. (2008) "La libertad sindical en la doctrina del Tribunal Constitucional", Revista del Ministerio de Trabajo y Asuntos Sociales, 73, 247-312. pp 308-309.

La libertad sindical responde la bien jurídico protegido de los trabajadores de defender sus intereses colectivos como tales trabajadores por cuenta ajena. De tal forma, que al proteger los datos relativos a la libertad sindical no tan solo se protege el bien jurídico del derecho a la libertad sindical sino también para la protección de datos personales, sobre su tratamiento, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados, sino como un derecho autónomo e independiente tal como ya se ha descrito en los tres puntos anteriores.

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado. El consentimiento del afectado no es tratado como un valor absoluto. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende autorizar su tratamiento.

1.7.5.5. Datos relativos al origen racial

Tratamiento por los textos legales: inicialmente en la Ley de 1992 aparece como datos del origen racial, en la Directiva de 1995 este término desaparece, para volver en 1999 y permanecer hasta 2018. A partir del año 1999 la expresión datos de origen racial se modifica por datos de origen racial o étnicos. La aparición de la conjunción "o" da a entender que son cosas distintas, los orígenes raciales y los orígenes étnicos, es decir, o son raciales o son étnicos.

Es obligado comentar que la expresión datos relativos a origen racial, ha sido muy criticada. Brevemente, tan solo hay que decir que científicos genetistas afirman que las razas no existen[40] lo cual ha sido recogido por la prensa internacional, BBC.Mundo.com de 18 de diciembre de 2002[41], El País de 13 de septiembre de 2000[42], incluso hay quienes dudan de la conveniencia de seguir utilizando la palabra raza, El País de 13 de febrero de 2016[43].

El Informe de la Reunión de Consulta sobre la Conferencia Mundial contra el Racismo, la Discriminación Racial, la Xenofobia y las Formas Conexas de Intolerancia, celebrada en Bellagio, Italia, del 24 al 28 de enero de 2000, manifiesta:

> "La inmensa mayoría de los expertos en la materia coincide en que, desde el punto de vista científico y antropológico, el concepto de que los seres humanos pueden dividirse y clasificarse definitivamente en distintas 'razas' carece de fundamento. No hay más que una raza: la raza humana".

[40] TEMPLETON AR. (2013) "Razas biológicas en humanos". Estudios en historia y filosofía de las ciencias biológicas y biomédicas vol. 44,3. 262-71 y CANN RL,, STONEKING, M., WILSON, AC. (1987). "Mitochondrial DNA and human evolution". Nature, International journal of science, 325, 31-36

[41] BBC.Mundo.com (18 de diciembre de 2002), "Las razas no existen" Disponible en http://news.bbc.co.uk/hi/spanish/science/newsid_2585000/2585667.stm (28/02/2021).

[42] ANGIER, N. (13 septiembre 2000) "La genética descalifica el concepto de raza". EL PAIS Disponible en https://elpais.com/diario/2000/09/13/futuro/968796001_850215.html (28/02/2021).

[43] MEDIAVILLA, J. (7 febrero 2016) "¿Debemos seguir empleando el concepto de raza"? EL PAIS Disponible en https://elpais.com/elpais/2016/02/05/ciencia/1454696080_059342.html (28/02/2021).

En relación con el debate del término raza, Directiva 2000/43/CE del Consejo, de 29 de junio de 2000, relativa a la aplicación del principio de igualdad de trato de las personas independientemente de su origen racial o étnico en su Considerando número seis dice que: "la Unión Europea rechaza las teorías que tratan de establecer la existencia de las razas humanas, añadiendo que el uso, en la presente Directiva, del término "origen racial" no implica el reconocimiento de dichas teorías." En relación con lo cual el Considerando número cincuenta y uno del Reglamento 2016/679 dice que

> "especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas".

La prohibición de la utilización de datos relativos al origen racial de las personas se basa en el artículo 2 de la Declaración Universal de los Derechos Humanos (DUDH), el cual reza: "Toda persona tiene los derechos y libertades proclamados en esta Declaración, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición". DUDH adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948.

La prohibición de la utilización de datos raciales de las personas también se basa en artículo 1 de la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial Adoptada y abierta a la firma y ratificación por la Asamblea General en su resolución 2106 A (XX), de 21 de diciembre de 1965; el artículo 2.2. de los Pactos de las Naciones Unidas de Derechos Civiles y Políticos y sobre Derechos Económicos, Sociales y Culturales adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966; en el principio de no discriminación del artículo 21 de La carta de los derechos fundamentales de la Unión Europea fue proclamado por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en Niza; y el artículo 21 de la Carta de derechos fundamentales de la Unión Europea, dice:

> "Artículo 21. No discriminación
>
> 1. Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual.
>
> 2. Se prohíbe toda discriminación por razón de nacionalidad en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea y del Tratado de la Unión Europea y sin perjuicio de las disposiciones particulares de dichos Tratados."

A estos artículos se suma el artículo 6 del Tratado de la Unión Europea, el cual dice:

"Artículo 6 (antiguo artículo 6 TUE)

1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados.

   Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados.

   Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones.

2. La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados.

3. Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales."

Por otra parte, en el ordenamiento jurídico español, la discriminación por cuestiones de raza no tan solo está prohibida por la Constitución de 1978 al afirmar su artículo 14 que todos los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social y sino también a través de su artículo 10 al proclamar que las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España. Los tratados ratificados por España sobre derechos y libertades más utilizados por el Tribunal Constitucional [44] son:

1. "Pacto internacional de Derechos Civiles y Políticos, hecho en Nueva York, adoptado por la resolución 2200 (XXI) de la Asamblea General de las Naciones Unidas, de 16 de diciembre de 1966. Instrumento de ratificación de 27 de abril de 1977. (BOE nº 103, de 30 de abril de 1977).
2. Protocolo facultativo del Pacto internacional de Derechos Civiles y Políticos, hecho en Nueva York, adoptado por la resolución 2200 (XXI) de la Asamblea General de las Naciones Unidas, de 16 de diciembre de 1966. Instrumento de adhesión de 25 de enero de 1985. (BOE nº 79, de 2 de abril de 1985).
3. Segundo Protocolo facultativo del Pacto internacional de Derechos Civiles y Políticos destinado a abolir la pena de muerte, hecho en Nueva York, adoptado por la resolución 44/128 de la Asamblea General de las Naciones Unidas, de 15 de

[44] MERINO NORVERTO, M. (2003) "Sinopsis artículo 10 de la Constitución Española" Congreso de los Diputados. Portal temático. Disponible en https://app.congreso.es/consti/constitucion/indice/sinopsis/ sinopsis.jsp?ar t=10&tipo=2 (31/01/2021); y SIEIRA, S. (2011) "Sinopsis artículo 10 de la Constitución Española" Congreso de los Diputados. Portal temático. Disponible en https://app.congreso.es/consti/ constitucion/ indice/ sinopsis/ sinopsis.jsp?art=10&tipo=2 (28/02/2021).

diciembre de 1989. Instrumento de ratificación de 11 de abril de 1991. (BOE nº 164, de 10 de julio de 1991).

4. Pacto internacional de Derechos Económicos, Sociales y Culturales, hecho en Nueva York, adoptado por la resolución 2200 A (XXI) de la Asamblea General de las Naciones Unidas, de 16 de diciembre de 1966. Instrumento de ratificación de 13 de abril de 1977. (BOE nº 103, de 30 de abril de 1977).
5. Convenio para la Prevención y la Sanción del Delito de Genocidio, hecho en Nueva York, adoptado por la resolución 260 A (III) de la Asamblea General de las Naciones Unidas, de 9 de diciembre de 1948. Instrumento de adhesión de 13 de septiembre de 1968. (BOE nº 34, de 8 de febrero de 1969).
6. Convención sobre el Estatuto de los Refugiados, hecha en Ginebra, adoptada por la Conferencia de Plenipotenciarios sobre el Estatuto de los Refugiados y de los Apátridas el 28 de julio de 1951. Instrumento de adhesión de 14 de agosto de 1978. (BOE nº 252, de 21 de octubre de 1978; corrección de errores en BOE nº 272, de 14 de noviembre de 1978).
7. Protocolo sobre el Estatuto de los Refugiados, hecho en Nueva York, el 31 de enero de 1967. Instrumento de adhesión de 14 de agosto de 1978. (BOE nº 252, de 21 de octubre de 1978).
8. Convención Internacional sobre la Eliminación de todas las formas de Discriminación Racial, hecha en Nueva York, adoptada por la resolución 2106 A (XX) de la Asamblea General de las Naciones Unidas, de 7 de marzo de 1966. Instrumento de adhesión de 13 de septiembre de 1968. (BOE nº 34, de 8 de febrero de 1969).
9. Convenio sobre los Derechos Políticos de la Mujer, adoptado en virtud de la resolución 640 (VII) de la Asamblea General de Naciones Unidas. Nueva York, 31 de marzo de 1953. Instrumento de adhesión de 14 de enero de 1974 (BOE nº 97, de 23 de abril de 1974); corrección de errores en BOE de 22 de agosto de 1974).
10. Convención sobre la Eliminación de todas las formas de Discriminación contra la Mujer, adoptada en virtud de la resolución 640 (VII) de la Asamblea General de Naciones Unidas. Nueva York, 31 de marzo de 1953. Instrumento de adhesión de 14 de enero de 1974 (BOE nº 97, de 23 de abril de 1974); corrección de errores en BOE de 22 de agosto de 1974).
11. Convención contra la tortura y otros tratos o penas crueles, inhumanos o degradantes, adoptada por la resolución 39/461 de la Asamblea General de Naciones Unidas el 10 de diciembre de 1984 en Nueva York. Instrumento de ratificación de 21 de octubre de 1987 (BOE nº 268, de 9 de noviembre de 1987).
12. Convención sobre los Derechos del Niño, adoptada por la resolución 44/25 de la Asamblea General de Naciones Unidas de 20 de noviembre de 1989 en Nueva York. Instrumento de ratificación de 6 de diciembre de 1990 (BOE nº 313, de 31 de diciembre de 1990). Bastantes sentencias del Tribunal Constitucional utilizan como parámetro interpretativo dicha convención, entre otras, STC 67/1998, de 18 de marzo (fundamento jurídico 5).
13. Los diversos Convenios de la Organización Internacional del Trabajo, que tienen una incidencia notable en el terreno de los derechos de los trabajadores.
14. Convenio para la protección de los Derechos Humanos y de las Libertades fundamentales, hecho en Roma el 4 de noviembre de 1950. Instrumento de ratificación de 26 de septiembre de 1979 (BOE nº 243, de 10 de octubre de 1979).

15. Protocolo Adicional al Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales, París, 20 de marzo de 1952. Instrumento de ratificación de 27 de noviembre de 1990 (BOE nº 11, de 12 de enero de 1991).
16. Protocolo número 6 al Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales relativo a la Abolición de la Pena de Muerte, hecho en Estrasburgo el 28 de abril de 1983. Instrumento de ratificación de 20 de diciembre de 1984 (BOE nº 92, de 17 de abril de 1985).
17. Carta Social Europea, hecha en Turín el 18 de octubre de 1961. Instrumento de ratificación de 29 de abril de 1980 (BOE nº 153, de 26 de junio de 1980). Se cita en pocas decisiones del Tribunal Constitucional y con escasa relevancia en la fundamentación jurídica. Entre otras STC 229/1992, de 14 de diciembre (fundamentos jurídicos 2 y 4)
18. Protocolo Adicional a la Carta Social Europea, hecho en Estrasburgo el 5 de mayo de 1988. Instrumento de ratificación de 7 de enero de 2000 (BOE nº 99, de 25 de abril de 2000, corrección de errores en BOE nº 220, de 13 de septiembre)."

En los puntos que tratan los datos relativos a la libertad ideológica, de religión, de creencias y de libertad sindical se ha defendido que la normativa de protección de datos actúa protegiendo dos puntos de vista, por una parte, su propio bien jurídico y por otra, el derecho autónomo del propio control del dato personal. Sin embargo, en este punto sobre los datos de origen racial no se puede argumentar la defensa de los dos escenarios aludidos.

El término raza no alude a ningún derecho directo, sino que además la Unión Europea elude y disculpa la utilización de dicho término.

En consecuencia, la protección del dato relativo al origen racial defiende por una parte, un bien jurídico ajeno al del concepto de raza, es decir, el bien de la igualdad frente a la ley y el bien jurídico de la no discriminación en las cuestiones alegadas por algunos en el contexto de la creencia de la división de la humanidad en varias razas y, por otra parte, protege el derecho autónomo e independiente del propio control sobre los datos personales de cada cual, tal como ya se ha descrito en los cuatro puntos anteriores.

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado. El consentimiento del afectado no es tratado como un valor absoluto. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende autorizar su tratamiento.

1.7.5.6. Datos relativos al origen étnico

Tratamiento por los textos legales: este término, origen étnico, aparece por primera vez en la Ley Orgánica de 1999 y se mantiene en los textos de 2016 y 2018.

El término etnia y étnico y todo lo que envuelve a la etnicidad, su significado y definición no se muestra pacífico en el colectivo científico y en los debates que sobre lo étnico se suscita entre los eruditos. La antropología contiene una subespecialidad denominada etnología, que es la ciencia social encargada de estudiar los diferentes pueblos y culturas

del mundo antiguo y actual, en cuanto a su cultura, sistemas y subsistemas económicos y de subsistencia, religión, creencias, arte, moral, derecho, costumbres, relaciones familiares parentescos, organización familiar, social, política y liderazgos. Para algunos autores antropología y etnología es lo mismo.

Etnia etimológicamente está formada por dos raíces griegas y significa "cualidad de un pueblo", siendo sus dos componentes léxicos "ethnos" (nación, pueblo, raza), más el sufijo "ia" (cualidad)[45]. Una definición reconocida de etnia la dio en 1983 Ronald J. L. Bretón diciendo que: "En un sentido amplio, la etnia se define como un grupo de individuos unidos por un complejo de caracteres comunes -antropológicos, lingüísticos, político-históricos, etc.- cuya asociación constituye un sistema propio, una estructura esencialmente cultural."[46]

GOMEZ GARCÍA[47], catedrático de filosófica de la Universidad de Granada, entiende que el concepto de etnia, desde un punto de vista académico, no se sostiene ni en su vertiente lingüista, ni en su vertiente basada en el parentesco, ni tan siquiera en la vertiente sustentada en las teorías de la tradición religiosa. El profesor de Granda mantiene que, si bien la cuestión de las tribus y sus derechos no tiene discusión, lo cierto es que los Estados modernos actuales han sido posibles gracias a integración política de la pluralidad social y se han sustentado en un escenario supratribal, en consecuencia, en los Estados modernos la etnicidad no tiene sentido e incluso es perjudicial para la propia sociedad, tal como se ha visto durante el siglo XX tanto en Europa como en ciertas regiones del continente africano.

La utilización del término etnia y de todo lo que ello conlleva no puede escaparse a la visión real de que ha habido abusos, maltratos y genocidios sobre lo que en algunos momentos de la historia de la sociedad actual se han entendido por etnias. Por otra parte, es conocida la desastrosa utilización que han hecho de la dinámica étnica algunos líderes políticos utilizando su liderazgo sobre grupos sociales o determinadas regiones de Europa. En la memoria colectiva occidental reciente está el desastre genocida de la Guerra de Bosnia (1992-1995) o el de Srebrenica en julio de 1995, creado a raíz de la manipulación política de grupos residentes en las regiones de Croacia, Serbia y Bosnia.

Frente a estas manifestaciones de orden científico hay que contrastar las de orden jurídico, a lo cual hay que añadir que el Tribunal Supremo a través de la STC 214/1991, de 11 de noviembre de 1991 no tan solo reconoce a las etnias, sino que le confiere el derecho al honor como grupo o raza, así:

> "El odio y el desprecio a todo un pueblo o a una etnia (a cualquier pueblo o a cualquier etnia) son incompatibles con el respeto a la dignidad humana, que sólo se cumple si se atribuye por igual a todo hombre, a toda etnia, a todos los pueblos. Por lo mismo, el derecho al honor de los miembros de un pueblo o etnia, en cuanto protege y expresa el sentimiento de la propia

[45] Diccionario etimológico español, 2020

[46] BRETON RJL. (1983) "Las etnias". Ed. Oikos-Tau. p 17.

[47] GÓMEZ GARCÍA P. (1998) "Las ilusiones de la identidad. La etnia como seudoconcepto". Gazeta de Antropología", 14, 13-15.

> dignidad, resulta, sin duda, lesionado cuando se ofende y desprecia genéricamente a todo un pueblo o raza, cualesquiera que sean".

En cualquier caso, sean los argumentos del origen que sean, en la memoria colectiva subyace la gravedad de los hechos que en torno al concepto etnia se han producido durante la historia de la humanidad, lo cual hace comprensible el esmero de la norma que tiene como fin la protección del tratamiento del dato personal en prevención de situaciones o actos que puedan dañar derechos fundamentales, ya no tan solo el de la intimidad y honor sino el de la protección de los propios datos personales.

Al hablar de los datos relativos a la libertad ideológica, de religión, de creencias y de libertad sindical se ha defendido que la normativa de protección de datos actúa protegiendo dos puntos de vista, por una parte, su propio bien jurídico y por otra, el derecho autónomo del propio control del dato personal. Sin embargo, cuando se ha abordado la protección del dato relativo al origen racial se han cambiado los marcos de referencia, manteniendo como común tan solo el derecho autónomo e independiente del propio control sobre los datos personales de cada cual, tal como ya se ha descrito en los cuatro puntos anteriores. Ahora, al referirnos a la protección del dato relativo a las etnias se vuelve a realizar una aproximación similar a la que se ha realizado en el caso del término raza. De tal forma, que se entiende que dicha protección se fundamenta en los mismos principios, por una parte, el derecho fundamental a la no discriminación y por el otro al del control propio sobre los datos personales.

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende autorizar su tratamiento.

1.7.5.7. Datos relativos a la vida sexual, orientación sexual o sexualidad

Tratamiento por los textos legales: inicialmente en la Ley de 1992 aparece como datos relativos a la vida sexual, en la Directiva de 1995 este término se cambia por sexualidad, en 1999 se vuelve a utilizar vida sexual para pasar al término orientación sexual en los años 2016 y 2018.

En este orden de cosas es preciso distinguir los conceptos orientación sexual del concepto identidad de género, pues mientras orientación sexual es relativo a la atracción entre personas, la identidad de género, independiente de la orientación sexual y del sexo biológico al nacimiento, es el concepto que se tiene cada cual como ser sexual y de los sentimientos que esto conlleva[48].

[48] MONEREO ATIENZA, C. (2 julio 2014) "Aproximación conceptual a la orientación sexual e identidad de género: estrategias político-jurídicas para la reivindicación de derechos del colectivo LGBT" Comunicación Congreso Universitario Internacional Investigación y Género (5º). Sevilla. Disponible en https://idus.us.es/bitstream/handle/11441/41135/Pages%20from%20Investigacion_Genero_14-2-5.pdf?sequence=1&isAllowed=y (31/01/2021).

El artículo 14 de la Constitución Española, hace a todos los españoles iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social. Recalcando que al decir "cualquier otra condición" incluye por descontado a cualquier condición de carácter sexual.

El artículo 2 de la DUDH proclama el derecho de toda persona a estar protegido por la DUHD sin discriminación ninguna y por ningún motivo.

El artículo 2 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) prohíbe la discriminación de las personas por cualquier motivo o circunstancia y proclama solemnemente la igualdad de todos frente a la ley y en concreto frente al PIDCP en los países que los suscriban. Por otra parte, los Principios de Yogyakarta son los principios sobre la aplicación de la legislación internacional de derechos humanos en relación con la orientación sexual y la identidad de géneros fue presentada el 26 de marzo de 2007 en el Consejo de Derechos Humanos de la ONU en Ginebra y ratificada por la Comisión Internacional de Juristas. La Comisión Internacional de Juristas (CIJ) es una Organización no gubernamental (ONG) internacional con sede en Ginebra (Suiza), creada en 1952 por Walter Linse, presidente de la Asociación de Juristas Alemanes Libres.

El concepto de intimidad es más amplio que el de privacidad, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de la personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor, una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes. Ambos, el derecho a la intimidad y al honor están presentes en el artículo 18 de la Constitución de 1978.

El derecho a la intimidad personal, al honor y a la propia imagen, reconocido por el artículo 18 de la Constitución Española se entiende protegidos, en cuanto al tratamiento de datos, por la normativa reguladora del tratamiento de los datos personales y contra los que se tipifican conductas delictivas en el Código Penal como delitos contra la liberad e indemnidad sexual (Titulo VIII) y delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (Titulo X).

Por otra parte, el Tribunal Constitucional reconoce como derecho fundamental primario como un derecho autónomo e independiente, el poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también

permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso[49].

En consecuencia, la normativa que protege estos datos lo hace no tan solo ante el bien jurídico del derecho fundamental de la libertad sexual el cual debe ser protegido por todo el abanico legislativo del ordenamiento jurídico, sino también para la protección de datos personales, sobre su tratamiento, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados, sino como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso[50].

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende autorizar su tratamiento.

1.7.5.8. Datos relativos a la salud

Tratamiento por los textos legales: lo datos relativos a la salud, inicialmente en la Ley de 1992 aparece dentro de artículo denominado datos especialmente protegidos, para luego entre 1995 y 2016 aparecen como datos dentro de las categorías especiales de datos. En el texto del año 2018, le Ley Orgánica 3/2018, no aparece explícitamente en el listado de categorías especiales de datos, si bien implícitamente vienen referidos en este artículo. En realidad, al ser el artículo 9 de la Ley Orgánica 3/2018 un artículo de mera remisión al Reglamento (UE) 2016/679 se entiende como incluido, aunque por otra parte el artículo 9 de la Ley Orgánica 3/2018 solo hace mención explícita a los datos relativos a ideología, a afiliación sindical, a religión, a orientación sexual, a creencias y a origen racial o étnico. En este orden de cosas, el artículo 9 de la Ley Orgánica 3/2018 tampoco incluye a los datos genéticos ni biométricos, sino que son tratados en las disposiciones adicionales de la Ley Orgánica 3/2018.

El tratamiento del dato personal relacionado con la salud de las personas está fuertemente regulado por el artículo 9 del Reglamento (UE) 2016/679, en su punto 1 mediante la prohibición de su tratamiento, en su punto 2 del artículo 9 mediante la exclusión en diez (10) supuestos.

Resumiendo, las excepciones son las que se aplican en el derecho, excepciones por causa de necesidad o cuando el bien jurídico a proteger es superior al desprotegido mediante la aplicación de la excepción, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 vienen a concretar los supuestos de esas excepciones.

[49] STC 292/2000, de 30 de noviembre (El Pleno), FJ 7º.

[50] se desprende de: STC 94/1998, de 4 de mayo (Sala segunda) FJ 6º y STC 292/2000, de 30 de noviembre (El Pleno) CG.

A este listado de exclusiones de la prohibición del tratamiento, punto 2 del artículo 9, se une la base jurídica para el tratamiento lícito en el punto 3 del mismo artículo 9.

En el punto 1 del capítulo 1 del Título III, se trata este punto en más profundidad con la denominación de "Los datos de relativos a la salud dentro del artículo 9 del Reglamento (UE) 2016/679, de Tratamiento de categorías especiales de datos personales".

El dato relativo a la salud es tratado por la Ley Orgánica 3/2018 en relación al artículo 9 del Reglamento (UE) 2016/679 también en la Disposición adicional decimoséptima. Esta disposición y su contenido se tratará en el punto 2 del apartado 2 del Capítulo 3 del Título III o capítulo 3.2.2 del Título III, de este trabajo de investigación dentro del análisis del régimen del Tratamiento de los datos.

1.7.5.9. Datos relativos a la genética

Tratamiento por los textos legales: los datos relativos a la genética son incluidos en el artículo 9.1 del Reglamento (UE) 2016/679 dentro de las Categorías especiales de datos, en este orden de cosas, el artículo 9 de la Ley Orgánica 3/2018 no incluye a los datos genéticos ni a los datos biométricos, sino que son tratados en las disposiciones adicionales de la Ley Orgánica 3/2018.

El Considerando 34 del Reglamento (UE) 2916/679 dice respecto al dato genética que debe entenderse como los datos personales relacionados con características genéticas, heredadas o adquiridas de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN) o del análisis de cualquier otro elemento que permita obtener información equivalente. El Considerando 35 incluye al dato genético dentro de los datos de salud cuando han sido obtenidos de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal.

El artículo 4 del Reglamento (UE) 2016/679 define datos genéticos como los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Por otra parte, el artículo 2 de la Declaración Internacional sobre los Datos Genéticos Humanos de 16 de octubre de 2003, de la Organización de las Naciones Unidas para la educación, la ciencia y la cultura, determina que datos genéticos humanos son información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos. A su vez el artículo 4, de la Declaración de octubre de 2003, reconoce la singularidad del dato genético en base a que pueden indicar predisposiciones genéticas de los individuos; a que pueden tener consecuencias importantes para la familia, comprendida la descendencia, y a veces para todo el grupo al que pertenezca la persona en cuestión, que se perpetúen durante generaciones; a que pueden contener información cuya relevancia no se conozca necesariamente en el momento de extraer las muestras biológicas; y a que pueden ser importantes desde el

punto de vista cultural para las personas o los grupos. En base a lo cual el mismo artículo determina que se debería prestar la debida atención al carácter sensible de los datos genéticos humanos e instituir un nivel de protección adecuado de esos datos y de las muestras biológicas.

La propia Declaración Internacional sobre los Datos Genéticos Humanos en su artículo 5 limita la finalidades de tratamiento de los datos genéticos humanos a los fines diagnóstico y asistencia sanitaria, lo cual incluye la realización de pruebas de cribado y predictivas; a la investigación médica y otras formas de investigación científica, comprendidos los estudios epidemiológicos, en especial los de genética de poblaciones, así como los estudios de carácter antropológico o arqueológico; a la medicina forense y procedimientos civiles o penales u otras actuaciones legales; a cualesquiera otros fines compatibles con la Declaración Universal sobre el Genoma Humano y los Derechos Humanos y el derecho internacional relativo a los derechos humanos.

En base a lo cual, dicha Declaración Universal, hace una serie de recomendaciones tales son las de la necesidad del consentimiento de la persona y el derecho a su revocación, el derecho a decidir no ser informado de los resultados de los estudios genéticos que se le realicen y derecho a recibir asesoramiento genético.

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado, libre, claro y explicito. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende autorizar su tratamiento.

Finalmente, esta importancia que el legislador le da a todo lo relativo con la genética se constata en España a través de la aprobación, promulgación y publicación de la Ley 14/2007, de 3 de julio, de Investigación biomédica. Esta ley determina que la salud y el bienestar de la persona que participe en un proceso de investigación biomédica estará por encima del interés de la sociedad o de la ciencia, en base al Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina, suscrito en Oviedo el día 4 de abril de 1997, y que entró en vigor en España el 1 de enero de 2000.

1.7.5.10. Datos biométricos o relativos a la biometría de las personas

Tratamiento por los textos legales: los datos biométricos son incluidos en el artículo 9.1 del Reglamento (UE) 2016/679 dentro de las categorías especiales de datos, en este orden de cosas, el artículo 9 de la Ley Orgánica 3/2018 no incluye a los datos biométricos, sino que son tratados a una Disposición adicional.

El Instituto Nacional de Ciberseguridad, sociedad estatal regulada por el Real Decreto Legislativo 1/2010 de 2 de julio, publicó en 2016 el documento “Tecnologías biométricas aplicadas a la ciberseguridad”, el cual permite resumir la biometría en los siguientes términos:

> "La biometría es un método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento. Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc.
>
> Las características biométricas empleadas deben tener las siguientes propiedades: universalidad: todos los individuos las tienen; singularidad o univocidad: distinguen a cada individuo; permanencia en el tiempo y en distintas condiciones ambientales; y medibles de forma cuantitativa.
>
> Fundamentalmente se distinguen dos grupos de tecnologías biométricas en función de la metodología utilizada: aquellas que analizan características fisiológicas de las personas y aquellas que analizan su comportamiento.
>
> Dentro de las tecnologías biométricas fisiologías existen el reconocimiento: de huella dactilar; facial; del iris; de la geometría de la mano; de la retina; vascular; líneas de la palma de la mano; forma de las orejas; piel, textura de la superficie dérmica; ADN, patrones personales en el genoma humano; composición química del olor corporal; entre otras.
>
> En cuanto a las Tecnologías biométricas de comportamiento en base al reconocimiento: de firma; de escritor de texto manuscrito; de voz; de escritura de teclado; de la forma de andar; entre otras."

El artículo 4 del Reglamento (UE) 2916/679 define datos biométricos como datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. Los videos se incluyen en este tipo de datos, excluyéndolos de la limitación de los datos domésticos[51].

En base al Considerando 51 Reglamento (UE) 2916/679 el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

La normativa protectora de los datos personales prohíbe su tratamiento y exige el consentimiento del afectado. En los textos del año 2016 y 2018, el legislador reduce en determinados casos el efecto del consentimiento del afectado condicionando su eficacia a la existencia de normas de la UE o de los Países miembros que prohíban el tratamiento de determinados datos especiales sobre los que se pretende autorizar su tratamiento.

1.8. El dato en el contexto de la legislación de protección de datos vigente en la UE

A pesar de ser un término familiar, cotidiano y de amplio uso, el concepto de dato no está definido en ninguno de los textos vigentes relativos a la protección de datos como se ha venido insistiendo en esta Tesis. En realidad, lo que está definido en la norma es

[51] AEPD (2019) Resolución de la Agencia Española de Protección de Datos R/00778/2018, de 20 de mayo de 2018.

el concepto de dato personal, concretamente los define el Reglamento (UE) en su artículo 4, apartado 1 diciendo que

> "datos personales: son toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

A pesar de que el término dato no esté definido, del análisis de la voz "dato" y sus expresiones semánticas que se exponen en el apartado 6 del Capítulo 1 del Título I, se puede deducir su definición, su uso o el significado que para este texto tiene el término dato. De tal forma se deduce:

1. en primer lugar, el término dato se aplica de forma desigual y en sentidos distintos en el sentido de lo que es un signo o señal que dice algo de alguna cosa o de alguna persona.
2. en segundo lugar, aparecen sentidos del término dato de carácter amplio y de carácter restrictivo, en ocasiones la norma trata el término dato sin acotación y en muchas otras ocasiones lo circunscribe, lo delimita o lo casa o une a otra expresión. La expresión dato exacto, da a entender que diferencia el dato exacto del inexacto, y que por cualquier motivo el legislador lo entiende suficientemente distinto como para que conste en la norma.
3. en tercer lugar, con facilidad el texto incluye en el término dato la calificación de contexto (aquella que se deduce por el contexto en el cual se ha utilizado el vocablo) de dato informático o dato digital o dato en un tratamiento automatizado.
4. en cuarto lugar, el dato suele confundirse con la información. Esta confusión es muy frecuente.
5. por último, también es cierto, que el conjunto de datos que no ofrecen información sobre la persona no son tributarios del control por parte el Reglamento (UE) 2016/679.

Igual ocurre al analizar el vocablo "dado" y su aplicación semántica en el texto de la Ley Orgánica 3/2018.

El texto del Reglamento (UE) define a la expresión dato personal y los confunde con la expresión información personal, que como ya se ha descrito, dato e información no son sinónimos[52].

El artículo 1 del Reglamento (UE) 2016/679 es el que determina "El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de

[52] *Vid. Supra p 30,* capítulo 1.3., del Título I.

tales datos". El dato al que se refiere es el dato de las personas físicas y en relación a su protección, más concretamente se refiere al tratamiento de dichos datos.

En el artículo 4 del Reglamento (UE) 2016/679 se define dato personal como "toda información sobre una persona física identificada o identificable («el interesado»)". A reglón seguido el Reglamento define lo que entiende por persona identificable. Aparece en este artículo un nuevo concepto relativo al dato, este es, "identificador", de tal forma que una persona física identificable será toda persona cuya identidad pueda determinarse mediante un identificador, como por ejemplo un nombre o un número de identificación.

Como ya se ha tratado, el dato relevante a efectos del Reglamento (UE) 2016/679 es el dato no anónimo, es el dato que permite identificar a personas. El dato que junto a otro genera información suficiente para identificar a una persona determinada en el presente, pasado o futuro.

En este contexto, para el Reglamento (UE) 2017/679, el dato es información, pues el dato o los datos que no generan información no son susceptibles de aplicarse a esta norma. Así pues, en el contexto de esta norma, dato no suele ser tan solo uno, sino que dato pertenece a varios datos juntos y por sí solos pueden generar información sobre la identidad de una persona, intemporalmente.

La normativa europea, tanto la derivada como la nacional, el sistema normativo del Consejo de Europa y las sentencias del Tribunal de Justicia de la Unión Europea, relativas a la protección de datos protegen el dato de las personas física y más concretamente protege a los derechos fundamentales de las personas físicas, protección de la vida privada, controlando el tratamiento de los datos que permiten identificarla[53].

El texto del Reglamento (UE) 2016/679 entiende, en su artículo 4, por tratamiento

> "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"

es decir, cualquier actividad humana sobre cualquier dato de cualquier persona.

En cuanto al ámbito de aplicación material de la protección del dato de las personas físicas corresponde, en base al artículo 2 del Reglamento (UE) 2016/679, "al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero." Así mismo, el Texto legal entiende por fichero en su artículo 4, "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya

[53] RUIZ MIGUEL C. (2003) "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico". Revista de Derecho Comunitario Europeo, 7 (14), 7-43.

sea centralizado, descentralizado o repartido de forma funcional o geográfica". Sin embargo, el Considerando 15 aclara que "A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas."

Con relación al ámbito territorial de la protección del dato de cualquier persona física amparado por el Reglamento (UE) 2016/679, en su artículo 3 determina que "el presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no", es decir, actividades que tengan que ver con la Unión independientemente de que se hagan dentro o fuera de la misma. Sin embargo, el responsable o encargado del tratamiento podrá no estar establecido en la Unión cuando su actividad de tratamiento esté relacionada con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago o el control de su comportamiento, en la medida en que este tenga lugar en la Unión, o cuando el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público, según el Considerando 80 del Reglamento (UE) 2016/679.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales añade en sus disposiciones generales (Título I) el Dato de la persona fallecida, en su artículo 3, tanto de personas mayores como menores de edad. En este orden de cosas se entiende que el Ley Orgánica no amplia el ámbito de la protección, sino que autoriza que los herederos o personas vinculadas de hecho con el fallecido puedan ejercer los derechos que le reconoce la ley en protección de datos en nombre del fallecido.

Capítulo 2. El derecho fundamental a la protección de datos

2.1. Antecedentes

Referirse a los derechos fundamentales y entender su naturaleza requiere hacer un breve apunte sobre su origen. Los derechos y deberes fundamentales son un concepto histórico[54].

Tal y como afirma VALCERDE MENDEZ, la gran aportación de la Modernidad tras el Renacimiento es la idea del individuo como persona en su óptica singular, mediante el descubrimiento de lo individual, una gran aportación del racionalismo del siglo XVII y XVIII[55]. Estas corrientes del pensamiento se suman a la presión que ejerce la nueva burguesía, así pues, "a partir del siglo XVII en Gran Bretaña, y del XVIII en Francia, en el resto de Europa y en las colonias inglesas de América del Norte, la fuerza de la burguesía le llevará a reclamar la participación en ese poder político"[56].

Este nacimiento de la idea de la persona y el deseo de control y participación del poder del Estado, hace que en Inglaterra en 1689 se apruebe Bill of Rights (Carta de Derechos) por imposición del Parlamento inglés al príncipe Guillermo de Orange como condición para la sucesión al rey Jacobo II. A este acontecimiento histórico le siguen la Declaración de Independencia de los Estados Unidos (1776), las Declaraciones de los Derechos del Hombre y del Ciudadano (1789, 1793 y 1795), la Constitución de La I Republica Austriaca (1920), y finalmente la Ley Fundamental de Bon (1949), representando este proceso la constitucionalización de los derechos convirtiéndolos en derechos fundamentales[57].

El origen iusnaturalista de los derechos fundamentales es reconocido por la dogmática, así como su culminación en la ilustración con un destacado papel de la escuela de juristas de Salamanca y en especial de Votira, Soto, Vázquez de Menchana y Suarez[58].

2.2. Cuestiones Preliminares

La RAE define al derecho fundamental como aquel "derecho declarado por la Constitución que goza de máximo nivel de protección". Por otra parte, los derechos fundamentales han salido calificados como aquellos inherentes al ser humano y que pertenecen a cada persona por el hecho de serlo. Están íntimamente relacionados a los derechos humanos, diferenciándose para algunos autores básicamente en su ámbito de

[54] PECES BARBA, G. "Derechos Fundamentales". p 8. Disponible en https://e-archivo.uc3m.es/bitstream/handle/10016/10462/derechos_Peces;jsessionid=A8CC67612F2D8A33739CDC759A2E49E5?sequence=1 (28/02/2021).

[55] VILLAVERDE MENEDEZ, I. (2015) "Los derechos fundamentales en la historia. Una aproximación a su origen y fundamento". En CARBONELL SANCHEZ et Al "Estado constitucional, derechos humanos, justicia y vida universitaria". Estudios en homenaje a Jorge Carpizo. Derechos humanos, tomo V, vol. 2. (573-598). p 573.

[56] PECES BARBA, G. "Derechos …..", op.cit; p 12.

[57] CRUZ VILLALON, P. (1989) "Formación y evolución de los derechos Fundamentales". Revista Española de Derecho Constitucional, 29, 35-62. pp 46, 54-55, 62.

[58] De ESTEBAN, J. GONZALEZ-TREVIJANO, J. (1992) "Curso de Derecho Constitucional Español I". Madrid. Servicios de publicaciones facultad derecho Universidad Complutense de Madrid. Reimpresión 1994. p 261.

aplicación mientras que para otros son intercambiables[59]. En España los derechos fundamentales y los derechos humanos se vinculan a través de artículo 10 de la Constitución de 1978[60]. Los derechos humanos en base a la Declaración Universal de Derechos Humanos de la ONU tienen una serie de características esenciales: imprescriptibles, intransferibles, irrenunciables y universales, además son inalienables e indivisibles[61]. Sin embargo, la definición que nos brinda la ONU no ayuda especialmente a entrar y entender el concepto de derecho fundamental.

En este orden de cosas, para CRUZ VILLALON la *conexión de sentido*, concepto acuñado por HELLER[62] y que lo añade al concepto de contenido del derecho positivo, es la Constitución. En otras palabras, "los derechos fundamentales nacen con la Constitución y se acaban con la Constitución" , es decir, los derechos fundamentales son una categoría dogmática del derecho constitucional, de tal forma que "allí donde no hay Constitución no habrá derechos fundamentales" [63].

Esta constitucionalización de un derecho, acotado por una serie de exigencias o limitaciones que veremos más adelante, es decir, esta visión positivista de los derechos fundamentales para PECES-BARBA tiene un contrapeso iusnaturalista en su origen "los derechos fundamentales poseen una dimensión ética, que se convierte en eficaz con su

[59] AGUILAR CAVALLO, G. (2010) "Derechos fundamentales-derechos humanos. ¿Una distinción válida en el siglo XXI? Boletín Mexicano de derecho comparado, 43 (127), 15-70. pp 25-26.

[60] Artículo 10.2 de la Constitución de 1978: Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

[61] ONU (2016), "Derechos Humanos", Manual para Parlamentarios nº26. Oficina del Alto Comisionado. Naciones Unidad. Disponible en https://www.ohchr.org/ Documents/ Publications/ Handbook Parliamentarians_SP.pdf (31/01/2021).

[62] "La ciencia del sentido aísla el contenido de significación o sentido, e investiga la conexión de sentido en su legalidad específica, sin relación alguna en lo posible, con la "actualización" real." "Así, pues, la ciencia del sentido y la ciencia de la realidad, la jurisprudencia dogmática y la teoría del Estado, aparecen, tanto por sus objetos cuanto, por sus métodos, claramente separadas. No obstante, o justamente a causa de esta separación, cumple manifestar que la emancipación del conocimiento propio de las ciencias del sentido, respecto a la realidad social, no es jamás absoluta. Hemos distinguido entre conexiones de sentido lógicomatemáticas e históricas y no vamos ahora a examinar si esta distinción será, asimismo, sólo relativa. La separación de las conexiones de sentido históricas, y también de todas las jurídicas —que nunca son formas '"puras", sino que siempre aparecen condicionadas por la realidad—, respecto de su fundamento real y del sujeto de conocimiento, sólo es posible en una relativa medida; su conocimiento nunca puede ser, por tal motivo, "pura" ciencia del sentido."

"La conexión de sentido puede, en verdad, concebirse partiendo del "movimiento del pensamiento", que es relativamente autónoma, pero la forma social sólo puede serlo partiendo del movimiento del hombre que actúa como una constelación, constantemente cambiante, de fuerzas efectivas. En la estructura de sentido no acontece nada, es historia acontecida; en cambio, la formación social es historia que está sucediendo y operando. Las formaciones sociales son grupos de voluntad y, en ellos, la voluntad humana actúa como causa final; su estructura ideológica no excluye, en manera alguna, la causalidad, antes la tiene por base". HELLER, H. (1934) "Teoría del Estado" (Política Y Derecho) (Spanish Edition). Fondo de Cultura Económica. Edición de Kindle. Primera edición electrónica, 2015. Posición 1236 a 1240 y 1247 a 1264.

[63] CRUZ VILLALON, P. (1989) "Formación y evolución …..", op.cit; p 41.

incorporación al Derecho positivo con la intermediación del poder, que asume los mismos valores que los derechos representan y por esa razón impulsa su positivación" [64].

Estas exigencias y limitaciones que hacen que un derecho en un texto constitucional se convierta en derecho fundamental es básicamente su reserva de ley, orgánica u ordinaria según el caso[65], y el contenido esencial[66].

Los Derechos Fundamentales de la Constitución española de 1978 tienen plena fuerza normativa, vinculando a todos los poderes públicos, artículo 53.1 CE, incluso al legislador.

Estos derechos se regulan en el Título I de la Constitución española, "De los derechos y deberes fundamentales", y se pueden clasificar en tres tipos: 1. Derechos fundamentales y libertades públicas, artículos 14 a 29; 2. derechos fundamentales básicos, Derechos y deberes de los ciudadanos, artículo 30 a 38; 3. Derecho fundamentales informadores, Principios rectores de la política social y económica, artículo 39 a 52[67].

Para algunos autores los derechos fundamentales son los que constan entre el artículo 14 y el 38, concretamente esta postura es defendida por CRUZ VILLALON y por el Tribunal Constitucional[68], para otra corriente de la doctrina, de ESTEBAN, J. y GONZALEZ-TREVIJANO, los derechos fundamentales son todos lo comprendidos en el Titulo 1 de la

[64] PECES-BARBA, G. "Derechos Fundamentales". p 33. Disponible en https://e-archivo.uc3m.es/ bitstream/ handle/10016/10462/derechos_Peces;jsessionid= A8CC67612F2D8A33739CD C759A2E49 E5? sequence=1 (28/02/2021).

[65] De ESTEBAN, J. GONZALEZ-TREVIJANO, J. (1992) "Curso de Derecho Constitucional …..", op.cit; p 270.

[66] "En efecto, el hecho de que las diversas teorías acerca del contenido esencial de los derechos indaguen sobre cuál es el elemento normativo protegido no tiene como finalidad averiguar el parámetro de control de constitucionalidad, sino lisa y llanamente determinar en qué consisten los derechos fundamentales y, más concretamente, su ámbito irreductible" GAVARA DE CARA, JC (1994) "Derechos fundamentales y desarrollo legislativo. La garantía del contenido esencial de los derechos fundamentales en la Ley Fundamental de Bonn". Tesis doctoral. Universidad Autónoma de Barcelona. De 1 enero de 1994. Barcelona. España. p 212. Disponible en http://www.cepc.gob.es/Controls/Mav/getData.ashx?MAVqs=~aWQ9MzU1MzkmaWRlPTEwMzcmdXJsPTE1Jm5hbWU9UkNFQ18xOV8yMDkucGRmJmZpbGU9UkNFQ18xOV8yMDkucGRmJnRhYmxhPUFydGljdWxvJmNvbnRlbnQ9YXBwbGljYXRpb24vcGRm. (28/02/2021).

[67] De ESTEBAN, J. GONZALEZ-TREVIJANO, J. (1992) "Curso de Derecho Constitucional …..", op.cit; p 272.

[68] "Ello resulta lógicamente del doble carácter que tienen los derechos fundamentales. En primer lugar, los derechos fundamentales son derechos subjetivos, derechos de los individuos no sólo en cuanto derechos de los ciudadanos en sentido estricto, sino en cuanto garantizan un status jurídico o la libertad en un ámbito de la existencia. Pero al propio tiempo, son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado social de Derecho o el Estado social y democrático de Derecho, según la fórmula de nuestra Constitución (art. 1.1).

Esta doble naturaleza de los derechos fundamentales, desarrollada por la doctrina, se recoge en el art. 10.1 de la Constitución, a tenor del cual «la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la Ley y a los derechos de los demás son fundamentos del orden político y de la paz social». Se encuentran afirmaciones parecidas en el derecho comparado, y, en el plano internacional, la misma idea se expresa en la Declaración universal de derechos humanos (preámbulo, párrafo primero) y en el Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales del Consejo de Europa (preámbulo, párrafo cuarto)". STC 25/1981, de 14 de julio 1981 (El Pleno), FJ 5.

Constitución, es decir, del artículo 10 al 55. Para este sector de la doctrina, "serían así derechos fundamentales todos los regulados en la Norma Fundamental"; a lo que añaden "no cabe duda de que existe una graduación de la importancia de los derechos regulados en la Constitución" [69].

La cuestión de los derechos fundamentales de amplia o estricta delimitación dentro del Título I, no se agota con este Título I, sino que según de ESTEBAN, J. y GONZALEZ-TREVIJANO, la Constitución tiene algún fallo puesto que algunos de los derechos fundamentales se han regulado en otros títulos destinos al Título I[70].

La función que cumplen los derechos fundamentales en la estructura de la Constitución es establecer para los ciudadanos espacios de autodeterminación de la conducta, indisponibles a todos los poderes públicos. Se configuran, así como ámbitos de autodeterminación, de libertad subjetiva (dimensión subjetiva). Son origen inmediato de derechos y obligaciones y no meros principios programáticos[71].

Los derechos fundamentales también son componentes estructurales básicos del Ordenamiento jurídico debido a que son la expresión jurídica del sistema de valores que, por mandato del constituyente, artículo 10 CE, han de informar la organización jurídico-política.

Estos derechos, se configuran como principios o valores superiores del ordenamiento jurídico que imponen al Estado una obligación de actuar positivamente con el fin lograr que tales derechos sean reales y efectivos adoptando la regulación organizativa y procedimental necesaria para la efectividad del ejercicio de cada derecho fundamental (dimensión objetiva). Conforme a los artículos 9 y 53 CE, todos los poderes públicos, incluidas las diferentes Administraciones Públicas, se encuentran vinculados por los derechos fundamentales.

Los derechos fundamentales en el marco de nuestro Estado constitucional de derecho deben ser analizados teniendo en cuenta cuatro claves:

[69] De ESTEBAN, J. GONZALEZ-TREVIJANO, J. (1992) "Curso de Derecho Constitucional …..", op.cit; p 271.

[70] "Citemos como ejemplos el derecho de audiencia en el procedimiento de elaboración de disposiciones que afectan al ciudadano (artículo 105.a.), el derecho de acceso a archivos y registros administrativos (artículo 105.b), el derecho a la indemnización por lesiones sufridas en el funcionamiento de los servicios públicos (artículo 106.2), el derecho a la gratuidad de la justicia (artículo 119), el derecho a la indemnización por errores judiciales o por el funcionamiento anormal de la justicia (artículo 121), el derecho a ejercitar la acción popular (artículo 125) y, por último, el derecho a participar en al administración de la justicia por medio del jurado (artículo 125)" De ESTEBAN, J. GONZALEZ-TREVIJANO, J. (1992) "Curso de Derecho Constitucional …..", op.cit; p 269.

[71] VILLAVERDE MENEDEZ, I. (2007) "La función de los derechos fundamentales en el marco del Estado de las Autonomías" Revista d'Estudis Economics i Federals,4, 203-239. SSN**:** 1886-2632. p 215.

1.º Todos los derechos son limitados y además pueden entrar en conflicto unos con otros. No hay derechos fundaméntales absolutos[72]. El derecho a la vida puede así limitar el derecho a la protección de datos de carácter personal[73].

2.º La igualdad de valor y rango de todos los derechos fundamentales. Esta igualdad exige llevar a cabo en cada caso de conflictivo una ponderación[74].

3.º Las limitaciones de derechos fundamentales tienen que ser establecidas por normas con rango de Ley que han de respetar el contenido esencial de aquellos. Sólo así se garantiza que el Parlamento -los representantes de los ciudadanos- legitime democráticamente la limitación. En ningún caso es admisible que un Gobierno dicte normas de rango reglamentario para establecer con carácter general limitaciones de derechos[75].

4.º El régimen de los derechos fundamentales está reservado a la Ley Orgánica, es decir, a las Cortes Generales. Las comunidades autónomas no tienen competencia para establecer dicho régimen[76].

La tutela judicial de los derechos Fundamentals y las libertades públicas tal como establece el artículo 53.2 de la Constitución podrá ser recabada por cualquier ciudadano en cuanto a las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30.

> "la exigencia derivada del art. 53.2 de la C.E., en virtud del cual los procesos ordinarios de amparo han de estar presididos por los principios de "preferencia" y de "sumariedad". La preferencia implica prioridad absoluta por parte de las normas que regulan la competencia funcional o despacho de los asuntos; por sumariedad, como ha puesto de relieve la doctrina, no cabe acudir a su sentido técnico (pues los procesos de protección

[72] "Ahora bien, si los derechos no son absolutos, tampoco lo son sus límites, como nos recuerda, entre otras muchas, la Sentencia 254/1988 de 21 de diciembre, en su Fundamento Jurídico 3º" RUIZ RUIZ R. (2007) "La ponderación en la resolución de colisiones de derechos fundamentales. Especial referencia a las jurisprudencia constitucional española". Revista Telemática de Filosofía del Derecho, 10, 53-57. p 63.

[73] STC 96/2010, de 15 de noviembre (Sala Segunda), FJ 3º.

[74] SÁNCHEZ GONZÁLEZ, S. (2003) "De la imponderable ponderación y otras artes del Tribunal Constitucional". La Revista Teoría y Realidad Constitucional, 12-13, 351-382. p 364.

[75] VIDAL GIL, E. (2001) "La Interpretación de los Derechos Fundamentales por el Tribunal Constitucional". Anuari de dret parlamentari. 11, 73-112. p 93. Disponible en https://www.cortsvalencianes.es /sites/default/files/ media/file_author/73_0.pdf. (28/02/2021).

[76] CONSTITUCIÓN ESPAÑOLA. Artículo 53.1 CE. "Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a)."

Artículo 81 CE "1. Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución.

2.La aprobación, modificación o derogación de las leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto."

> jurisdiccional no son "sumarios", sino especiales), sino a su significación vulgar como equivalente a "rapidez". En definitiva, por proceso "sumario" tan solo cabe entender la exigencia constitucional de que los procesos de protección jurisdiccional sean sustancialmente rápidos o acelerados" [77].

El reconocimiento, el respeto y la protección de los otros principios reconocidos por el Título I de la Constitución, concretamente los que aparecen en el Capítulo tercero "De los principios rectores de la política social y económica" informarán la legislación positiva, la práctica judicial y la actuación de los poderes públicos. Mientras que sólo podrán ser alegados ante la Jurisdicción ordinaria de acuerdo con lo que dispongan las leyes que los desarrollen.

El marco jurídico de la protección de datos en España viene configurado básicamente por el Reglamento (UE) 2016/679 del Parlamento 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, en adelante, también RDPG), por la Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales y por todas aquellas leyes que le son de aplicación y en especial a las que se remite el RGPD para legitimar las excepciones de consentimiento exigidas por la propia norma.

En cuanto al sector sanitario, todas las leyes a las que se refiere la "Disposición adicional decimoséptima. Tratamientos de datos de salud" de la Ley Orgánica 3/2018, configurando en realidad un auténtico sistema normativo o sistema de protección de los datos relativos a la salud[78].

[77] STC 81/1992, de 28 de mayo de 1992 (Sala Primera). FJ 4º.c).

[78] Se crea un verdadero sistema de protección de los datos relativos a la salud a través de la Disposición adicional decimoséptima (Tratamientos de datos de salud) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Este sistema jurídico recoge las siguientes disposiciones:

1. La Ley 14/1986, de 25 de abril, General de Sanidad en: artículo 18.17; y artículo 55 bis.
2. La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales en: artículo 5.4; y artículo 22.4.
3. La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica en: artículo2.5; artículo 3; artículo 5; artículo 7; artículo 8.3; artículo 9; artículo 10; artículo 14; artículo 15; artículo 16; artículo 17; artículo 18; y artículo 19
4. La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud en: artículo 33.3; artículo 52; artículo 53; artículo 57; artículo 58; y artículo 79.
5. La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias en: artículo 4.9; artículo 4.10; y artículo 5.2.
6. La Ley 14/2007, de 3 de julio, de Investigación biomédica en: artículo 1; artículo 2.c); artículo 3; artículo 4.5; artículo 5; artículo 8; artículo 9.1; artículo 12.2.d); artículo 13; articulo 15.2.d); artículo 15.3; artículo 23; artículo 25.5; artículo 27.3; artículo 34.2.c); artículo 42.2; artículo 44; artículo 45; artículo 47; artículo 48; artículo 49; artículo 50; artículo 51; artículo 52; artículo 53; artículo 58; artículo 59; artículo 66; artículo 67; artículo 69.6; y artículo 70.1.
7. La Ley 33/2011, de 4 de octubre, General de Salud Pública en: artículo 7.2; artículo 9.1; artículo 41.2; y artículo 41.3.

El Considerando 2 del Reglamento (UE) 2016/679, en relación a los principios que defiende, empieza diciendo:

> "los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas. Aunque el Considerando 4 añade que el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad."

El preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales dice:

> "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno."

Ante la realidad dual del derecho fundamental a la protección de datos personales contenido en el art. 18. 4 CE y el contenido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, ha defendido RALLO LOMBARTE

> "la convivencia del art. 8 de la Carta de Derechos Fundamentales de la Unión Europea y del art. 18.4 de la Constitución Española está pacíficamente garantizada por vía hermenéutica en la medida en que el derecho fundamental garantizado por el art. 18.4 de la Constitución Española va a ser directa y principalmente regulado por el Reglamento General de Protección de Datos, desplazándose el canon de protección del derecho fundamental a la interpretación que del art. 8 de la Carta de Derechos Fundamentales de la Unión Europea haga el Tribunal de Justicia de la Unión Europea"[79] .

En esta materia, como en tantos otros ámbitos, el legislador nacional ha visto desplazada su esfera de potestad normativa en favor de la potestad normativa del legislador

8. La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, en: artículo 99.
9. El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio, en: artículo 17; y artículo 19.4.
10. El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre en: artículo 92; y artículo 104.

[79] RALLO LOMBARTE, A. "El nuevo derecho de protección de datos", en "Revista española de derecho constitucional", año Nº 39, Nº 116. Ed. Centro de Estudios Políticos y Constitucionales, Madrid, 2019, pp. 58-59.

europeo, la propia Exposición de Motivos de la Ley Orgánica 3/2018 ha querido aclarar la compatibilidad entre ambas normas introduciendo una cierta idea de subsidiariedad y de complementariedad al indicar que

> "no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate".

Sin embargo, en el caso del derecho fundamental a la protección de datos, vemos que la realidad práctica determina que los aspectos que habitualmente deberían ser objeto de ley orgánica, como ocurre con la definición del derecho, con la configuración de su contenido esencial y con la articulación de sus límites, son, realmente, cuestiones reguladas por la normativa comunitaria. La Ley Orgánica 3/2018 se ha limitado a desarrollar las cuestiones específicas para las que el Reglamento Europeo remite a la normativa nacional y a incluir ciertas reiteraciones de preceptos del Reglamento, amén de tratar sobre materias que no recaen propiamente bajo una necesidad de ley orgánica, como es la regulación del régimen jurídico de la Autoridad de control o la llamativa inclusión del régimen de derechos digitales.

Para finalizar este punto sobre los aspectos preliminares del derecho fundamental de la protección de datos cabe mencionar que los Derechos Fundamentales que constan en la Carta de Derechos Fundamentales de la Unión Europea no son equiparables en todo a los derechos fundamentales entendidos como los derechos constitucionalizados, si bien las garantías son muy similares[80]. En este aspecto la Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa en 2019 (ADFUE) entiende que la limitación de estos Derechos Fundamentales está sometidos a reserva de ley, respeto al contenido esencial, los criterios de necesidad y proporcionalidad, así como el objetivo del interés general[81]. El ámbito de aplicación de la Carta de Derechos Fundamentales es aplicable solo al Derecho de la Unión, de tal forma el artículo 51[82], dice a tenor literal:

[80] El autor, PASCUA MATEO, en relación a la STC 76/2019m de 29 de mayo, en el recurso de inconstitucionalidad número 1405-2019, en su F.J. 3, dice: "se encarga de recordar la postura del Tribunal respecto de la aplicación de las normas del Derecho de la Unión relativas a los derechos fundamentales: son un instrumento interpretativo de los derechos constitucionales ex artículo 10.2 CE, pero además producen efectos directos sobre el ordenamiento. Su uso por el Tribunal se va a limitar al primer aspecto, puesto que, como viene señalando desde la STC 28/1991, el control de compatibilidad del derecho interno con el de la Unión es de mera legalidad y en ningún caso de constitucionalidad (véase también STC 140/2018, citada en la Sentencia). Como es bien sabido, esa posición, algo más difícil de sostener cuando se trata de enjuiciar el respeto a un derecho de la Carta de Derechos Fundamentales" PASCUA MATEO, F.A. (2019) "Un nuevo capítulo en la tutela del derecho a la protección de datos personales: los datos de contenido político. Comentario a la Sentencia del Tribunal Constitucional 76/2019, de 29 de mayo, en el recurso de inconstitucionalidad núm. 1405-2019 (BOE núm.151, 25 de junio de 2019", Revista de las Cortes Generales, 106, 549-558. p 554.

[81] ADFUE (2018) "Manual de legislación europea en protección de datos". Luxemburgo: Oficina de Publicaciones de la Unión Europea. Disponible https://op.europa.eu/es/publication-detail/-/publication/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1/language-es (28/02/2021).

[82] UE (7 diciembre 2000) "Carta de los Derechos Fundamentales de la Unión Europea" de (2010/C 83/02). C 83/402. Disponible en https://www.boe.es/doue/2010/083/Z00389-00403.pdf.

> "1. Las disposiciones de la presente Carta están dirigidas a las instituciones, órganos y organismos de la Unión, dentro del respeto del principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias y dentro de los límites de las competencias que los Tratados atribuyen a la Unión.
>
> 2. La presente Carta no amplía el ámbito de aplicación del Derecho de la Unión más allá de las competencias de la Unión, ni crea ninguna competencia o misión nuevas para la Unión, ni modifica las competencias y misiones definidas en los Tratados."

2.3. Derecho fundamental de la Protección de datos en la Constitución española de 1978

Independiente del preámbulo de la Ley Orgánica 3/2018 y del artículo 18 de la CE, el Considerando primero del Reglamento 2016/679, hace mención a que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental en base al artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y al artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) que establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Tales derechos fundamentales son mencionados también en el preámbulo de la Ley Orgánica 3/2018, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea.

El derecho a la protección de datos es un derecho fundamental en base al Considerando 1 del Reglamento 2016/679, al artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea y en especial en base al artículo 18 de la Constitución Española y a la STC 94/1988, entre otras sentencias.

El derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos[83].

El derecho fundamental a la protección de datos llamado frecuentemente derecho de autodeterminado informativa nace, según MARTINEZ MARTINEZ, de la sentencia del Tribunal Constitucional Alemán (TCFA) sobre la Ley del Censo. El autor refleja en su artículo la definición que hace de dicho concepto el TCFA[84], la cual se transpone

> "La autodeterminación del individuo presupone –también en las condiciones de las técnicas modernas de tratamiento de la información– que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada.
>
> Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no sólo tener conocimiento de que otros

[83] AEPD (2004) Guía "El derecho fundamental a la protección de datos de carácter personal". Agencia Española de Protección de Datos. p 6.

[84] MARTINEZ MARTINEZ. R. (2007) "El derecho fundamental a la protección de datos: perspectivas", Revista d'Internet, Dret i Politica, 5, 47-61. Disponible en http://idp.uoc.edu. p 48 (28/02/2021).

> procesan informaciones relativas a su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación."

Para SÁNCHEZ-ESCRIBANO la autodeterminación informativa es "el derecho de toda persona a decidir acerca de la difusión y utilización de sus datos personales sin otra limitación que la derivada de Ley y a través de la cual se pretenda salvaguardar un interés superior"[85].

La Constitución española en su Sección 1.ª De los derechos fundamentales y de las libertades públicas, del Capítulo segundo. Derechos y libertades, del Título I. De los derechos y deberes fundamentales, en su artículo 18.4 dice: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos." Ya reflejado en la Constitución Portuguesa de abril de 1976.

El Tribunal Constitucional en su sentencia STC 94/1998 señaló que[86]:

> "Este no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la "privacidad" según el neologismo que reza en la Exposición de Motivos de la L.O.R.T.A.D.-, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios."

En este orden de cosas, ELVIRA PERALES y GONZALEZ ESCUDERO insisten en la calificación de derecho fundamental independiente afirmando[87]:

> "Una primera interpretación llevó a considerar este derecho como una especificación del derecho a la intimidad, pero el Tribunal Constitucional ha interpretado que se trata de un derecho independiente, aunque obviamente estrechamente relacionado con aquél (SSTC 254/1993, de 20 de julio y 290/2000, de 30 de noviembre). El TC además señaló la vinculación directa de este derecho para los poderes públicos sin necesidad de desarrollo normativo (STC 254/1993)"

Hasta el año 2000 los derechos a la intimidad y a la protección de datos habían estado íntimamente ligados, aunque lo cierto es que el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona, mientras el derecho de la protección de datos se refiere a todo tipo de datos, sean íntimos o no[88]. A partir de la STC 292/2000 el TC define el contenido del

[85] MONTSERRAT SÁNCHEZ-ESCRIBANO, MI. (2015) "Libertad informativa y protección de datos: desarrollo de la jurisprudencia del Tribunal Constitucional y tutela penal en el delito de descubrimiento y revelación de secretos". Anuario Iberoamericano de Justicia Constitucional, 19, 323-363.

[86] STC 94/1998, de 24 de mayo (Sala segunda), FJ 6º.

[87] ELVIRA PERALES, A. (2006), "Sinopsis artículo 18 de la Constitución Española". Congreso de los Diputados. Portal temático. Disponible en http://www.congreso.es/consti/constitucion/indice/ sinopsis/sinopsis.jsp?art=18&tipo=2 (28/02/2021); y GONZÁLEZ ESCUDERO, A. (2011), "Sinopsis artículo 18 de la Constitución Española". Congreso de los Diputados. Portal temático. Disponible en http://www.congreso.es/consti/constitucion/indice/ sinopsis/ sinopsis.jsp?art=18&tipo=2 (28/02/2021).

[88] STC 292/2000, de 30 de noviembre (El Pleno) FJ6.

derecho fundamental a la protección de datos, convirtiéndolo en un derecho fundamental autónomo e independiente del derecho a la intimidad.

A todo lo cual, hay que añadir la protección a la intimidad que realiza en España el Código Penal, concretamente en su artículo 197 perteneciente al capítulo primero (del descubrimiento y revelación de secretos) del Título X de delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Este artículo en su punto 2 tipifica los abusos informáticos sobre datos personales, automatizados o no, y el acceso, utilización o alteración de cualquier medio de datos reservados de carácter personal[89].

Sin duda la doctrina ha debatido intensamente sobre este nuevo derecho fundamental a la protección de datos. Desde el punto de vista de un derecho de la personalidad, el bien jurídicamente protegido que tutela no es tan solo preservar oculta la vida privada sino la garantía de una plena capacidad para el desarrollo de la propia personalidad individual y el ejercicio de sus derechos, impidiendo la instrumentalización del ser humano. Desde el punto de vista positivo este nuevo derecho se sustenta en los debates parlamentarios en torno al artículo 18.4, la definición actualizada del concepto de intimidad y por último la nueva naturaleza de los bienes jurídicos implicados en las nuevas formas de comunicación. El bien jurídico tutelado excede de la esfera íntima de la persona garantizando otros valores y libertades, alcanzando el orden institucional con nuevos órganos de control y nuevos procedimientos para la tutela de los nuevos derechos[90].

Y con esto, nos adentramos en la dimensión subjetiva y objetiva del derecho fundamental a la protección de datos de carácter personal, y ha de señalarse que en este derecho la dimensión objetiva toma especial relevancia. Sin esta concepción objetiva no se podría construir el derecho a la protección de datos sobre unas reglas de tratamiento que conforman un orden jurídico encaminado al equilibrio entre los legítimos intereses en el tratamiento de datos y las facultades individuales que delimitan el contenido del derecho fundamental, esto es, dirigido a la justicia. Así, el propio artículo 18.4 CE señala una limitación en el uso de la informática a través de la ley como medio para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. No existe, pues, meramente un derecho subjetivo constitucional al honor y la intimidad personal y familiar, sino que, además, se consagra un derecho del individuo frente al Estado para que se limite legislativamente el uso de la informática. Y, ¿cuál podría ser el alcance de esa limitación? Para responder a esta pregunta, desde un punto de vista teórico, debemos acudir a los principios de idoneidad, necesidad y proporcionalidad, conforme a la teoría de los principios de Robert Alexy[91]. Pero, más allá de la vinculación con estos principios, la teorización de la vertiente objetiva de los derechos fundamentales encuentra en la organización y procedimiento "un medio -posiblemente el único existente- para producir un resultado acorde con los

[89] GÓMEZ NAVAJAS J. (2008) "La protección de datos personales en el Código Penal español". Revista Jurídica de Castilla y León,16, 325-372. p 333.

[90] HERRANZ ORTIZ, AI (2003) "El derecho a la protección de datos en la sociedad de la información". Bilbao. Instituto de Derecho Humanos. Universidad de Deusto. pp 17-18.

[91] ALEXY, R. (1993) "Teoría de los Derechos Fundamentales". Ed. Centro de Estudios Políticos y Constitucionales, Madrid, Madrid, 1993, 1ª edición, pp. 101-103.

derechos fundamentales y, con ello, asegurar eficazmente los derechos fundamentales en vista de la problemática moderna"[92].

Y, todo ello, teniendo presente la especial preponderancia que atribuye el Tribunal Constitucional a la protección de datos personales, así en la STC 76/2019[93], afirma que garantizar el derecho a la protección de datos de carácter personal garantiza nuestra democracia. Así en este orden de cosas, HELLER va más lejos entendiendo al derecho fundamental como uno de los dos pilares del Estado de Derecho limitando al poder político de los dirigentes, diciendo que "la organización de democrática del Estado de Derecho, con su división de poderes y garantía de los derechos fundamentales, limita eficazmente el poder político de los dirigentes"[94].

La convivencia de las normas es una de las cuestiones más relevantes del Estado de Derecho. En el ámbito de los derechos fundamentales esta complejidad ya fue resaltada por el profesor de Turín, Norberto BOBBIO, al decir "Son bien pocos los derechos considerados fundamentales que no se encuentran en concurrencia con otros derechos considerados también como fundamentales, y que no impongan, por tanto, en ciertas situaciones y respecto a particulares categorías de destinatarios"[95]. Lo cual ha pretendido ser explicado por el rasgo pluralista, característico de las constituciones de la segunda mitad del siglo XX[96]. Sin embargo, tal como dice PEREZ LUÑO en España es

> "el Tribunal Constitucional el que actúa como interprete supremo (artículo 1 Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional) y su interpretación de los preceptos constitucionales, es decir, la definición de la norma se impone a todos los poderes públicos» (STC de 26 de enero de 1981, en BJC, 1981, n. 2, p. 116)"[97].

No cabe duda de que entre los derechos fundamentales caben colisiones, y entre estos y los bienes jurídicamente protegidos, y en especial, entre el derecho fundamental de la protección de datos y el resto de los derechos fundamentales del Capítulo segundo. Los Derechos y libertades, del Título I de la Constitución pueden entrar y de hecho entran en colisión, en especial el bien jurídicamente protegido de la salud del artículo 43 de la Constitución.

La resolución de conflictos entre derechos fundamentales entre sí o con bienes jurídicamente protegidos se debe afrontar desde dos planos perfectamente

[92] HESSE, K (1978) "Bestand und Bedeutung der Grundrechte in der Bundesrepublik Deutschland", en "Euro päische Grundrechte-Zeitschrift" -5-, H. 19-22. Ed. N.P. Engel Verlag, Kehl am Rhein (Alemania). p 434.

[93] STC 76/2019, de 22 de mayo (El Pleno) AN 5º.

[94] HELLER H. (1934) "Teoría del Estado" México. Ed. Fondo de cultura económica. Decimosegunda reimpresión 1987. pp 266, 293.

[95] BAQUERIZO MINUCHE, J. (2009) "Colisión de los Derechos Fundamentales y juicio de ponderación". Revista jurídica. pp19-52 Disponible en https://www.revistajuridicaonline.com/wp-content/ uploads/ 2009/07/1-colision-derechos.pdf (28/02/2021). p 21.

[96] PINO, G. (2009) "Conflictos entre derechos fundamentales. Una crítica a Luigi Ferrajoli". DOXA, Cuadernos de Filosofía del Derecho, 32, 647-664. p 649.

[97] PÉREZ LUÑO, (1984) "Los derechos fundamentales". Editorial Tecnos. ebook edición Kindle de 2013. Posición 873 a 874.

diferenciables: el plano normativo o ámbito de regulación y el plano en la aplicación del Derecho (de las normas vigentes)[98].

2.3.1. En el ámbito de regulación

Hablamos del ámbito de la regulación, en este escenario de los derechos fundamentales, al referirnos al plano legislativo como función el poder legislativo en el marco del Estado, pero no en el de las Comunidades Autónomas.

Ese ámbito, en España, en lo relativo a los derechos fundamentales presenta tres garantías, la primera es la reserva de Ley (art. 53.1 CE y art. 81 CE, que determina que tiene que ser regulado por Ley Orgánica), lo cual no excluye una cierta participación reglamentaria siempre y cuando esta sea claramente subordinada a la ley[99], en segundo lugar, y muy vinculado a la anterior, la jerarquía normativa, en el sentido de que la ley solo y exclusivamente se puede modificar mediante otra ley y en tercer lugar, la salvaguarda del contenido esencial del derecho fundamental, por el legislador[100].

2.3.1.1. Garantías del derecho fundamental de la protección de datos en el marco de la Constitución

2.3.1.1.1. La reserva de ley en la regulación de la regulación del derecho a la protección de datos

La Constitución española de 1978 mediante los artículos 53.1 y 81 CE determina una garantía, reserva de Ley, para la regulación de cada uno de los derechos fundamentales del Capítulo II del Título I, tanto en su vertiente esencial y como en sus límites. Los derechos reconocidos en el Capítulo III del Título I, como el derecho a la protección de la salud, no están sometidos a esa reserva de Ley.

Toda intromisión del Estado en el marco de los derechos fundamentales y también en el ámbito de las libertades públicas que suponga su acotación o modificación o desarrollo (artículo 81.1 CE, Ley Orgánica) o module u obstaculice su ejercicio (artículo 53.1 CE, Ley Ordinaria, estatal o autonómica en función de la competencia material artículos 148 y 149 CE), precisa, en especial, lo que se entiende como una habilitación legal [101].

En este orden de cosas, la reserva de Ley es un requisito que garantiza formal y materialmente la seguridad jurídica de determinados aspectos fundamentales de la convivencia social en el Estado de Derecho. Sin duda, todo lo relativo a los derechos fundamentales y las libertades públicas se entiende como de vital importancia para la sociedad y en consecuencia la Constitución protege y ampara. Así pues, tan solo puede ser el poder legislativo y no el poder ejecutivo, el que entienda sobre esta materia

[98] RODRÍGUEZ-CHAVES MIMBRERO, B. (2020) "Salud versus privacidad: ¿podemos conservar ambas? Unos apuntes sobre la gestión de la pandemia por covid-19 desde los ámbitos de la regulación y aplicación del derecho". En BERMÚDEZ SANCHEZ J., DE MARCOS FERNÁNDEZ A. et al en "Transparencia, lobbies y protección de Datos" Madrid, Editorial Thomson Reuters. pp 542-543.

[99] SSTC 83/1984 (El Pleno) en FJ 3 y FJ5, 111/2014 (El Pleno) en FJ 4 y 139/2016 (El Pleno) en FJ 1, FJ 6 y FJ 7.

[100] STC 76/2019 (El Pleno) en FJ 2, FJ 5, FJ 6 y FJ 8.

[101] STC 14/2014, de 30 de enero (El Pleno).

constitucional y debe hacerlo mediante una Ley con el objeto de proteger a la persona de la arbitrariedad o la improvisación[102].

El Tribunal Constitucional no se ha inhibido de su papel y responsabilidad y en cuanto ha podido ha entrado a recordar al poder legislativo el marco en el que debe moverse al tener que respetar la reserva de ley que la Constitución obliga, en cuanto a la protección de datos personales. Así pues, este TC en su Sentencia 76/2019[103], [104] concreta las exigencias que debe respetar el legislador en la reserva de ley[105].

Desde la perspectiva de la Administración, la primera garantía de los derechos fundamentales frente a la Administración pública es el respeto a la reserva de Ley, a la que se superpone el respeto al principio de legalidad. Ello supone la ilegalidad de cualquier regulación adoptada por la Administración (estatal, autonómica o local) que carezca de la necesaria cobertura legal que afecte a un derecho fundamental.

La reserva de ley en la Constitución española se fundamenta en los siguientes tres principios[106] (criterios reiterados en varias sentencias[107]):

1. Garantizar que la modulación de "ámbitos de libertad que corresponden a los ciudadanos dependa exclusivamente de la voluntad de sus representantes, por lo que tales ámbitos han de quedar exentos de la acción del ejecutivo y de sus productos normativos propios, que son los reglamentos".

2. No limita o imposibilita que las leyes se remitan a normas reglamentarias para su complemento. No obstante, lo realmente importante es que se imposibilita "que tales remisiones hagan posible una regulación independiente y no claramente subordinada a la ley", lo que supondría una subversión de la reserva de ley constitucional a favor del poder legislador [108].

   En este orden de cosas, la STC 292/2000 declara inconstitucional el apartado 1 del art. 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, por permitir que una norma reglamentaria autorice la cesión de datos entre Administraciones públicas sin necesidad de recabar previamente el consentimiento del interesado.

[102] PEREZ LUÑO, (1984) "Los derechos …..", op.cit; posición 613.

[103] STC 76/2019, de 22 de mayo (El Pleno) FJ 5º.

[104] POLO ROCA, A., (2019) "Protección de datos y elaboración de perfiles: el nuevo artículo 58.bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general", Revista Galega de Administración pública (REGAP), 58, 507-527. p 523.

[105] "El enjuiciamiento constitucional que nos demanda la impugnación central se circunscribe, pues, a resolver si el legislador ha vulnerado la reserva de ley y el contenido esencial del derecho fundamental a la protección de datos personales (art. 18.4 CE en conexión con el art. 53. l CE), por renunciar a establecer el marco en el que se habilita el tratamiento, la finalidad del mismo y las garantías adecuadas frente al concreto uso de la informática previsto en la norma impugnada". STC 76/2019 de 22 de mayo de 2019 (El Pleno). FJ 2º.

[106] STC 83/1984, de 24 de julio (El Pleno), FJ 3º y FJ 4º.

[107] STC 111/2014, de 26 de junio (EL Pleno), FJ 2º y FJ 4º y STC 139/2016, de 21 de julio (El Pleno), FJ 6º.

[108] STC 83/1984, de 24 de julio (El Pleno), FJ 3º y FJ 4º; y STC 292/2000, de 30 de noviembre, (El Pleno), FJ 18º.

La reserva de ley implica no sólo la necesidad de una ley previa, sino que tal ley contenga un mínimo contenido material, sin que quepa una remisión en blanco al reglamento. Por ello, la remisión a la potestad reglamentaria para la fijación de esa regulación del contenido esencial debe reputarse inconstitucional.

3. El contenido legal necesario depende de la materia y del ámbito de las remisiones de la Constitución a la ley. Así, las SSTS de 5 de noviembre de 1999 sintetizan el significado de dicha reserva, señalando que en la Constitución "no hay una concepción global de la reserva de ley, sino reservas de ley en las que tal contenido tiene un alcance diverso, adquiriendo su máxima exigencia en relación con los derechos fundamentales y con el diseño constitucional básico de los poderes del Estado". Esta argumentación jurisprudencial se utiliza en la constitucionalidad de las leyes en relación con sus remisiones reglamentarias, que deben respetar, en todo caso, el principio de reserva de ley, y también en el control de los reglamentos.

En este sentido la STC 76/2019[109] sienta los siguientes parámetros que tiene que cumplir la disposición legal para que respete la reserva de Ley, estos son:

1.º finalidad del tratamiento de datos personales, sin que baste por sí sola la genérica mención al "interés público"[110].

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

3.º Debe establecer las garantías adecuadas para proteger los derechos fundamentales afectados. Y, desde luego, "la previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal[111] del tratamiento de datos personales de que se trate (mediante normas reglamentarias o de incluso normas de rango inferior al reglamentario, como una Circular o Instrucción)[112].

4.º Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado" (FFJJ 7º y 8º).

De ninguna manera basta con una remisión implícita al RGPD y a la Ley Orgánica 3/2018. Tampoco puede ser colmada por el titular de una potestad normativa

[109] STC 76/2019, de 22 de mayo, (El Pleno), FJ 5º.

[110] STC 76/2019, de 22 de mayo, (El Pleno), FJ 7º.

[111] MENÉNDEZ REXACH, A. (2003) "Ley y Reglamento en España", en Rosado Pacheco, S. (coord..): Derecho Europeo Comparado sobre Ley y Reglamento, pp93-210, Madrid, Centro de Estudios Ramón Areces. pp 93 a 119 y 193 a 196.

[112] En el caso enjuiciado por la STC, se aprobó la Circular 1/2019 por parte de la AEPD, que, en palabras del TC en STC 76/2019 en ningún caso puede colmar la insuficiencia legal del precepto impugnado.

limitada como es la Agencia Española de Protección de Datos o mediante una interpretación conforme[113].

5.º Finalmente, una remisión implícita tampoco resultaría coherente con el marco regulador europeo. No puede admitirse una hipotética remisión al Reglamento Europeo y a la nueva Ley Orgánica de Protección de Datos, pues esto equivaldría a una "remisión en blanco"[114] que dejaría en manos del Gobierno o bien, en ausencia de este último, del aplicador del derecho, la determinación de cuáles de las garantías previstas en ambas normas de remisión resultan aplicables al tratamiento en cuestión.

En conclusión, en materia de protección de datos de carácter personal la STC 76/2019 es muy clara y de manera exhaustiva señala que el artículo 18.4 en concordancia con el 53.1 CE exige la suficiente adecuación de la norma legal a los criterios de:

a) certeza en la Recopilación y tratamiento de los datos personales
b) la determinación de la finalidad del tratamiento
c) la existencia de las garantías adecuadas o las mínimas exigibles por la Ley

2.3.1.1.2. Jerarquía normativa

El sistema normativo se compone de diferentes normas por lo que resulta fundamental identificar los principios de relación entre ellas. La Constitución española de 1978 en su artículo 9.3 garantiza varios principios, entre los cuáles está el de la jerarquía normativa.

Los métodos, en el plano de la regulación legislativa, para la resolución del conflicto normativo son, por una parte, la aplicación la reserva de ley, ya visto, y, por la otra, el principio de la jerarquía normativa, y ambas van de la mano. Las normas que componen el ordenamiento jurídico no son de la misma clase, ni tienen la misma relevancia ni se aplican sobre el mismo ámbito. Para determinar cuándo se aplica cada una, es necesario acudir a su organización jerárquica de las diferentes fuentes y normas[115].

En base a la pirámide de Kelsen en la cúspide se sitúa la Constitución, le siguen las leyes orgánicas y especiales, a estas las leyes ordinarias y decretos ley, seguidas de reglamentos y ordenanzas y finalmente las sentencias[116].

El principio de jerarquía normativa exige analizar las distintas fuentes del Derecho, en España, la primera es la Constitución Española a la cual le siguen los Reglamentos y directivas de la Unión Europea que sean directamente aplicables, Tratados

[113] La técnica de la "interpretación conforme" no es admisible pues no estamos ante "varias interpretaciones posibles igualmente razonables", sino ante la insuficiencia de regulación detectada en una norma de desarrollo de un derecho fundamental. STC 76/2019, de 22 de mayo, (El Pleno), FJ 8ª.c).iii).

[114] STC 76/2019, de 22 de mayo, (El Pleno), FJ 8ª.c).i).

[115] ITURRALDE SESMA, V. (1999) "Sobre el concepto de jerarquía normativa". Anales de la Cátedra Francisco Suárez, 33, 261-277. p 262.

[116] KELSEN, H. (1960) "Teoría pura del Derecho". Buenos Aires. Editorial Universitaria de Buenos Aires. 4º Ed. 9ª reedición, 2009. pp 118-128.

internacionales ratificados por el Estado español, Leyes, emanadas de las Cortes Generales, leyes orgánicas y leyes ordinarias, normas con rango de ley, emanadas del Gobierno, Real Decreto Ley y Real Decreto Legislativo, los Reglamentos dictados por el Gobierno[117] y Administración Pública, con la forma jurídica de reales decretos, órdenes ministeriales [118].

A efectos de la ley y el reglamento, destacan dos principios fundamentales de relación, por una parte, el principio de jerarquía normativa (artículo 128.2 de Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas LPAC) y, por otra parte, el principio de competencia. Este último establece la distribución competencial entre Estado, Comunidades Autónomas y entes locales, así como de las diversas atribuciones de los órganos dentro de una persona jurídica[119].

El Código Civil[120], en su artículo 1.2, determina que una norma de rango inferior no puede contradecir ni vulnerar lo que establezca una de rango superior. Como complemento, el artículo 6 de la Ley Orgánica 6/1985[121] ordena que los Jueces y Tribunales no aplicarán los Reglamentos o cualquier otra disposición contraria a la Constitución, a la ley o al principio de jerarquía normativa. El principio de jerarquía normativa se complementa, por un lado, con el principio de temporalidad y por otro lado con el principio de especialidad.

En cuanto a la articulación entre la ley y el reglamento, además del principio de reserva de ley, se pueden destacar los siguientes criterios generales que conectan con el principio de jerarquía normativa, de tal forma que el reglamento no puede[122]:

1. modificar lo establecido en la ley (STS de 5 de diciembre de 1998, Ar. 9513, anula un precepto por modificar la definición del hecho imponible de un tributo establecida en la ley)[123]
2. ser menos exigente que la regulación legal[124] ni más restrictivo que ella[125].
3. dejar de regular un extremo que la ley ordena que sea regulado[126]

Por último, como no podría ser de otra forma, la Unión Europea tiene su propia jerarquía de las normas que en ella se producen e incluso en relación a las normas internas de los

[117] artículo 97 CE y Artículo 4 y 5 de la Ley del Goneron

[118] UNIR. "Descubre en qué consiste el principio de jerarquía normativa en el ámbito jurídico, sus características y de qué forma se configura en España". Revista UNIR. Disponible en https://www.unir.net/ derecho/ revista/ jerarquia-normativa/ (28/02/2021).

[119] MARCOS FERNÁNDEZ, A. et al (2018) "Fundamentos del Derecho Administrativo". Madrid. Servicio de Publicaciones de la Universidad Autónoma de Madrid. pp 97-100.

[120] Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

[121] Ley Orgánica del Poder Judicial de 1 de julio de 1985.

[122] Marcos Fernández, A. et al (2018) "Fundamentos del …..", op.cit; pp 97-100.

[123] STS 7315/1998 de 5 de diciembre (Sala de lo Contencioso), FD 4º.

[124] STS 898/1998 de 12 de febrero de 1998 (Sala de lo Contencioso), FD 3º.

[125] STS 9378/2000 de 19 de diciembre de 2000 (Sala de lo Contencioso), FD 2º y 4º.

[126] STS 7543/1998 de 14 de diciembre de 1998 (Sala de lo Contencioso), FD 2º.

países miembros, dicho orden normativo aparece en los artículos 288 y 296 del Tratado de Funcionamiento de la Unión Europea[127].

2.3.2.2.3. Contenido esencial

Tal como se ha descrito hasta ahora, para la resolución del conflicto normativo en el plano legislativo es de aplicación la reserva de ley, ya visto, y el principio de la jerarquía normativa, también visto. A estas dos se suma el respeto al contenido esencial[128].

El Tribunal Constitucional ha dictado en varias ocasiones que los derechos fundamentales no son ilimitados[129], por otra parte, nace del sentido lógico de las cosas pues sería una situación contradictoria de que el Ordenamiento Jurídico, cuya misión es limitar la conducta de la vida en sociedad, establezca instituciones jurídicas sin límites.

Siendo el Ordenamiento Jurídico un mapa de coordenadas, en unos casos estas coordenadas, límites, son fijados directamente por la propia Constitución[130], mientras que en otros casos se contienen en la ley que regula el derecho fundamental o en otra Ley que limite el contenido de este derecho.

La constitucionalidad de tales coordenadas, límites, viene expresada por la doctrina en dos tendencias. Una, la teoría absoluta, que defiende que el contenido esencial, artículo 53.1 CE, es el núcleo irreductible y no caben injerencias. La otra, es la teoría relativa del contenido esencial que radica en que esas injerencias son posibles siempre y cuando se trate de defender un bien, derecho o valor constitucional y respetando el principio de proporcionalidad ampliamente entendido, que engloba la adecuación, la necesidad y la proporcionalidad en sentido estricto[131].

Así pues, entramos en el terreno de la ponderación en la regulación del derecho (ponderación por el legislador) y que no hay que confundir con la ponderación en la aplicación del derecho.

Las garantías que impone el artículo 53.1 CE a la preservación de los derechos fundamentales obliga al poder legislativo a una serie de condicionamientos más rigurosos y limitativos que los habituales que encuentre dicho poder en otras cuestiones materiales sin una especial protección. La posibilidad de ponderar por parte del legislador para establecer límites a los derechos fundamentales está estrictamente condicionada. Como consecuencia de la ponderación se podrá dotar de límites a un derecho fundamental cuando estos sean justificados por la necesidad de dar

[127] EUR Lex. "Jerarquía de normas de la Unión Europea (UE)" Web oficial de la Unión Europea Disponible en https://eur-lex.europa.eu/summary/glossary/%20norms_hierarchy.html?locale=es (31/01/2021).

[128] STC 76/2019, de 22 de mayo (El Pleno), FJ 2º.

[129] STC 96/2010, de 15 de noviembre (Segunda sala), FJ 3º.

[130] Un ejemplo de ellos es el supuesto del artículo 18 CE, "inviolabilidad del domicilio, salvo existencia de un delito flagrante".

[131] GARRIZOSA PRIETO, E. (2004), "El principio de proporcionalidad como mecanismo de control de las injerencias en el derecho de huelga". Revista andaluza de trabajo y bienestar social, 77, 83-123. pp 90-91.

prevalencia, en determinadas circunstancias, al derecho, bien o principio constitucional que se encuentra en contraposición con aquél[132].

Por otra parte, es constitucionalmente obligado que la decisión del legislador, por la que se establezca límites a un derecho fundamental, sea ponderada o equilibrada. Esto es, la decisión a la que aquí se alude ha de cumplir con lo que se ha denominado "ley de ponderación", la cual entiende que cuanto mayor sea el grado de perjuicio del derecho fundamental de que se trate, mayor ha de ser la importancia del cumplimiento del bien, derecho o principio contrapuesto[133].

Ahora bien, hay que conjugar la exigencia de la *ley de la ponderación* con otra exigencia, esta es el *respeto al contenido esencial*, de tal forma que las limitaciones establecidas por la Ley, sean estas las que sean, en ningún caso pueden afectar al contenido esencial del derecho fundamental. Mas aun, el concepto de contenido esencial está conformado por aquella parte del derecho que es ineludiblemente necesaria para que su titular pueda satisfacer los intereses para cuya consecución el derecho se otorga[134].

En este sentido, la STC 112/2006[135] define el contenido esencial como

> "aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos. De este modo, se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección (STC 11/1981, de 8 de abril, FJ 10)" (STC 37/1987, de 26 de marzo, FJ 2)".

El contenido esencial de un derecho fundamental es su titularidad, objeto, contenido y límites[136]. En el caso del derecho a la protección de datos de carácter personal, artículo 18 CE, la Sentencia del Tribunal Constitucional de 2019[137] ha fijado con precisión cual es el alcance del contenido esencial del derecho a la protección de datos de carácter personal. En este sentido la Sentencia de Tribunal Constitucional de 2000[138], determina que consiste en un "poder de disposición y de control sobre los datos personales" y que tiene "una doble perspectiva":

[132] MEDINA GUERRERO, M. (1996) "La vinculación negativa del legislador a los derechos fundamentales". Madrid, McGraw-Hill Interamericana de España. pp 71,72, 75, 89 y 115. Vid. STC 120/1990, de 27 de junio, FJ 8 y STC 57/1994, de 28 de febrero, FJ 6.

[133] RODRÍGUEZ DE SANTIAGO, JM. (2000) "La ponderación de bienes e intereses en el Derecho administrativo". Madrid. Marcial Pons. p 61.

[134] STC 101/1991 de 13 de mayo (El Pleno), FJ 2º.

[135] STC 112/2006 de 5 de abril (El Pleno), FJ 10º.

[136] BASTIDA, FJ, ET AL (2004), "Teoría general de los derechos fundamentales en la Constitución Española de 1978". Madrid. Editorial Tecnos. pp 119-126.

[137] STC 76/2019 de 22 de mayo (El Pleno), FJ 6º.

[138] STC 292/2000 de 30 de noviembre (El Pleno), FJ 7º.

1. El artículo 18.4 CE no solo "consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona[139]
2. Un derecho instrumental ordenado a la protección de otros derechos fundamentales, esto es, "un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos[140]".

Concretando, los límites que sujeten un derecho fundamental han de respetar al menos dos requisitos:

a. debe responder a un fin constitucionalmente legítimo o encaminarse a la protección o la salvaguarda de un bien constitucionalmente relevante
b. precisa una habilitación legal, ya incida directamente sobre su desarrollo, artículo 81.1 CE, o ya limita o condiciona su ejercicio, artículo. 53.1 CE.

Es pues necesario que una ley defina los límites de los derechos y en particular del derecho a la protección de datos. Pero esta ley, para cumplir con el principio de seguridad jurídica, debe cumplir al menos dos exigencias:

I. previsibilidad[141]
II. certeza[142]

El control sobre la limitación a que se puede someter al contenido esencial de un derecho fundamental ha sido también interpretado por el Tribunal de Justicia de la Unión Europea en la sentencia Digital Rights Ireland Ltd y Kärntner Landesregierung sobre la función legislativa del Parlamento Europeo y del Consejo. Concretamente la STJUE de 8 de abril de 2024 contra la Directiva 2006/24/CE se basa en la vulneración de los Derechos de la Carta de Derechos Fundamentales de la Unión Europea. En esta sentencia el TJUE dice "Con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley, respetar su contenido esencial"[143].

El TJUE, incluso, limita la utilización del criterio del interés general para limitar el contenido esencial de un derecho fundamental de tal forma que entiende que el interés general por sí solo no es suficiente para cualquier limitación de contenido esencial de un derecho fundamental[144].

[139] SSTC 11/1998 de 13 de enero (Sala primera), FJ 5º; 96/2012 de 7 de mayo (Sala primera), FJ 6º; y 151/2014 de 25 de septiembre (El Pleno), FJ 7º.

[140] STC 292/2000, de 30 de septiembre (El Pleno), FJ 5º.

[141] STC 46/1990, de 15 de marzo (El Pleno), FJ 4º.

[142] STC 27/1981, de 20 de julio (El Pleno), FJ 10º.

[143] STJUE de 8 de abril de 2014 (Gran Sala) (asuntos C-293/12 y C-594/12), apartado 38. p 17.

[144] "En cuanto al carácter necesario de la conservación de datos que impone la Directiva 2006/24, ha de señalarse que es cierto que la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación. Sin embargo, este objetivo de interés general, por fundamental que sea, no puede por sí solo justificar que una

El contenido del derecho a la protección de datos personales incorpora un poder de disposición y control sobre los datos personales, que constituye parte del contenido del derecho fundamental a la protección de datos, y se concreta jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso y usos posibles, por un tercero, sea el Estado o un particular. Ello supone que la recogida y posterior tratamiento de los datos de carácter personal se ha de fundamentar en el consentimiento de su titular, facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional, de modo que esa limitación esté justificada, sea proporcionada y, además, se establezca por Ley.[145]

2.3.2.En la aplicación del derecho

"La aplicación del derecho significa un tránsito desde una regla general a una decisión particular o, como dice Kelsen, de una grada superior a una grada inferior, y el proceso espiritual que acompaña a la aplicación es la interpretación"[146].

El profesor DIEZ-PICAZO entiende por aplicación del derecho aquel conjunto de actividades llevadas a cabo para ajustar la realidad social a los dictados de las normas jurídicas[147]. Mientras que para PECES-BARBA es la utilización de la interpretación dada a una norma[148].

Los conflictos normativos en la aplicación de las normas han venido auxiliados por criterios de jerarquía, cronología y especialidad. Sin embargo, cuando la colisión ocurre dentro de un mismo cuerpo normativo, en el caso de los derechos fundamentales llamadas antonimias, los criterios generales no son útiles[149].

Los derechos fundamentales son normas distintas del resto de normas del ordenamiento jurídico funcionando como principios, siendo el procedimiento de la ponderación uno de los que permite resolver dichos conflictos y no el razonamiento subsuntivo[150],

medida de conservación como la establecida por la Directiva 2006/24 se considere necesaria a los efectos de dicha lucha." STJUE de 8 de abril de 2014 (Gran Sala) (asuntos C-293/12 y C-594/12), apartado 51, p 19.

[145] STC 17/2013, de 31 de enero (El Pleno), FJ 4º.

[146] ESPUNY VIDAL, MC. (2003), "La aplicación del derecho". A parte rei. Revista de filosofía del derecho, 25, 1-7.

[147] DIEZ-PICAZO, L, GULLÓN, A. (1997), "Sistema de derecho civil. Volumen I". Madrid. Editorial Tecnos. 9ª edición revisada. p 159.

[148] PECES-BARBA G. et Al (1999) "Curso de teoría del derecho". Madrid. Editorial Marcial Pons. IBSN: 84-7248-703-2. p 232.

[149] BAQUERIZO MINUCHE, J. (2009) "Colisión de los Derechos …..", op.cit; p 18.

[150] El profesor CABRA APALATEGUI realiza una minuciosa clasificación de las posibles antinomias de los derechos fundamentales en la trascripción de la ponencia del Encuentro entre la Universidad de Oviedo y la Universidad Autónoma de México. Los conflictos entre normas de derecho fundamental se suelen calificar como antinomias en concreto, también denominadas contingentes o externas, por contraposición a concepción clásica de las antinomias entre reglas o antinomias en abstracto. Introduce la clasificación de Antinomias genéricas, Antinomias Contextuales y Conflictos de instanciación. Las antinomias contextuales son las que no responden a inconsistencias del sistema jurídico, pero, a diferencias de estas, no son dependientes de las circunstancias empíricas. Así, los conflictos entre normas de derecho fundamental son definidos como conflictos en abstracto no derivables de inconsistencias del sistema jurídico. CABRA APALATEGUI, JM. (12 de diciembre 2016), "¿Antinomias constitucionales? Una concepción coherentista de las normas de derecho fundamental". Actas del III Coloquio Binacional

entendiendo por subsunción, RAE, la operación lógica que consiste en determinar que un hecho jurídico reproduce la hipótesis contenida en una norma general.

En este orden de cosas, existen unos mecanismos jurídicos para la resolución del conflicto entre el derecho fundamental de la protección de datos y otros derechos fundamentales o bienes jurídicamente protegidos dentro de la Constitución española. Los dos mecanismos utilizados, aunque no los únicos, son la ponderación y la proporcionalidad que para una parte de la doctrina son procedimientos alternativos y para otra parte de la doctrina son concurrentes[151].

2.3.2.1. Mecanismos jurídicos para la resolución del Conflicto en los casos en los que el derecho fundamental de la Protección de datos entre en conflicto con otros derechos fundamentales u otro bien jurídicamente protegido en el marco Constitucional

El artículo 53 de la Constitución española de 1978 establece que solo una ley orgánica pueda regular los derechos fundamentales, capítulo 2 del Título I, respetando el contenido esencial y que su tutela les corresponde a los tribunales ordinarios y al Tribunal Constitucional. De esta forma el legislador, y, en segundo término, los Tribunales ordinarios son los que pueden delimitar los derechos fundamentales y libertades públicas. Sin embargo, el Tribunal Constitucional ha sido quien se ha encargado de esta regulación, así pues, hay que acudir a la doctrina constitucional para conocer la extensión y límites de un derecho fundamental[152].

La expresión conflicto entre derechos fundamentales debe entenderse como el que surge entre el derecho y sus límites. Entendiendo que los derechos fundamentales de terceros marcan o establecen los límites de los derechos de otros[153].

Cuando se plantea un conflicto entre dos bienes jurídicamente protegidos o entre dos derechos fundamentales la resolución de este conflicto se debe afrontar desde dos planos perfectamente diferenciables: el plano normativo y el plano en la aplicación del Derecho (normas vigentes) [154]. En el caso de este capítulo, se verá más adelante que se enfrentan varios derechos, entre los cuales se encuentran, por un aparte, el derecho a la protección de datos de carácter personal, artículo 18 CE, y, por otra parte, el derecho a la protección de la salud, artículo 43 CE.

México-España en encuentro en la Universidad de Oviedo con la Universidad Autónoma de México "Derechos y obligaciones en el Estado de Derecho" de 12 a 15 de diciembre. p 257.

[151] "Así, mientras que algunos autores sostienen que el juicio de ponderación consiste en una sucesión de estadios entre los que se encuentran los diversos elementos que integran el principio de proporcionalidad, también es habitual afirmar que el control de proporcionalidad culmina con el test de la proporcionalidad en sentido estricto, en el marco del cual se realizaría propiamente la ponderación" (p 15). ARROYO JIMÉNEZ, L. (2009), "Ponderación, proporcionalidad y Derecho administrativo" InDret. Revista para el análisis del derecho, 2, 2-32. p 15.

[152] BANACLOCHE PALAO, J. (2018), "El desarrollo de los derechos fundamentales por el poder legislativo, el poder judicial y el tribunal constitucional" Estudios de Deusto. Universidad de Deusto. 66 (2). 17-46. p 45.

[153] BASTIDA, FJ, ET AL (2004), "Teoría general …..", op.cit; pp 113-115.

[154] RODRÍGUEZ-CHAVES MIMBRERO, B. (2020) "Salud versus privacidad: …..", op.cit; p 543.

Así pues, los planos de análisis frente al conflicto normativo serán realizados desde dos planos. Por una parte, desde el Plano normativo y, por otra parte, desde el Plano de la aplicación del Derecho vigente.

Desde el plano normativo (en nuestro supuesto, regulación del derecho a la protección de datos) se debe contemplar una serie de las claves, estas son, por una parte, el rango normativo de la norma que regula el derecho fundamental: reserva de Ley[155], se admite la colaboración reglamentaria siempre que sea claramente dependiente y subordinada a la ley[156]; jerarquía normativa: el reglamento no puede modificar lo establecido en la ley; y por último, la otra clave es el respeto al contenido esencial del derecho fundamental, por parte del legislador[157].

Desde el plano de la aplicación de la ley, se aplica dos criterios. Por una parte, el criterio del principio de la ponderación y, por otra parte, el del principio de la proporcionalidad.

2.3.2.1.1. La teoría de la ponderación y la proporcionalidad

En puntos anteriores se ha visto el plano normativo dentro de temática relativa a la resolución del conflicto normativo. En el marco de resolución del conflicto de normas destaca las relativas al plano de aplicación del derecho vigente, utilizando para ello tanto el juicio de proporcionalidad y como el de la ponderación[158].

La ponderación exigida a los órganos aplicativos del derecho presenta francas diferencias con respecto a la que se impone al legislador.

La aplicación de una determinada norma puede conllevar un conflicto con otras normas o derechos, en cuyo caso la Administración puede limitar uno de esos derechos en favor del otro, siempre y cuando se haga mediante un juicio de ponderación. Toda medida, acto o resolución, que restrinja algún derecho fundamental debe tener presente y asegurar que dichas limitaciones cumplan dos requisitos, una, que sea necesaria, la otra, que sea proporcional. De esta forma, por una parte, las medidas limitadoras deberán ser necesarias para conseguir el fin perseguido[159] y, por otra parte, estas limitaciones han de respetar equilibradamente la "proporcionalidad entre el sacrificio del derecho y la situación en que se halla aquel a quien se le impone"[160].

Concretamente, "la finalidad de la ponderación como respuesta al conflicto o tensión de derechos en concreto, es la ordenación de los derechos en cuestión"[161].

La exigencia de ponderación a los Gobiernos y las Administraciones Públicas implica la obligación de ejercer una motivación racional de sus decisiones. Motivación que además

[155] art. 53.1 CE y art. 81 CE, que determina que tiene que ser regulado por Ley Orgánica

[156] STC 83/1984 de 24 de julio (El Pleno), FJ 4º; STC 111/2014, de 26 de junio (El Pleno), FJ 4º; y STC 139/2016, de 21 de julio (El Pleno), FJ 8º.

[157] STC 76/2019, de 22 de mayo (El Pleno), FJ 6º.

[158] ARROYO JIMÉNEZ, L. (2009), "Ponderación, proporcionalidad …..", op.cit; pp 14-18.

[159] STC 62/1982, de 15 de octubre (Sala primera), FJ 5º.

[160] STC 37/1989, de 15 de febrero (Sala primera), FJ 7º.

[161] BAQUERIZO MINUCHE, J. (2009) "Colisión de los Derechos …..", op.cit; p 18. p 36, 2º párrafo.

debe ser estructurada en el cumplimiento de una serie de pasos, viniendo a entenderse como "ponderación como procedimiento" en el que hay que explicitar los principios en conflicto, atribuir importancia a cada uno de ellos conforme a una correcta argumentación que debe recogerse en el correspondiente acto jurídico-público como fundamentación.

La falta del requisito formal de la ponderación (ponderación como procedimiento) dentro de la aplicación del derecho vulnera el derecho fundamental, debiendo de ser, además, esta aplicación motivada explicitando las tres fases del procedimiento[162].

La ponderación es un método en el que se procede a través de tres fases sucesivas:

1ª. Identificación. Se identifican los principios (valores, bienes, intereses) en conflicto. "La regla de oro de la ponderación". Deberán evitarse los falsos problemas de la ponderación mediante una adecuada identificación de los principios en conflicto.

2ª. Valoración. Se atribuye a cada uno de ellos la importancia que le corresponda, según las circunstancias del caso. Lo que se ponderan son los principios, derechos, valores o intereses protegidos por el ordenamiento, de tal forma que los hechos, como tales, ni se ponderan ni pueden ponderarse. Aunque sí se pueden utilizar para dar prevalencia a un derecho o a un interés (apoyo normativo) sobre otro.

3ª. Priorización. Se otorga prevalencia a uno/s sobre el otro/s. Juicio de proporcionalidad en sentido estricto. Decisión de prevalencia conforme al criterio de que "cuanto mayor sea el grado de perjuicio a uno de los principios mayor ha de ser la importancia del cumplimiento de su contrario".

   Como resultado de cada ponderación es posible formular una regla de prevalencia condicionada. Esta regla permite un cierto grado de generalización o abstracción que facilita su aplicación a futuros conflictos planteados en términos semejantes a los del caso que se acaba de resolver, siempre que los hechos no sean sustancialmente distintos.

Por otra parte, el principio de proporcionalidad requiere que cualquier decisión que afecte a los derechos fundamentales sea la estrictamente indispensable. Estos tres subprincipios se enunciaron por primera vez en la STC 66/1995[163], en base a la cual se entiende que toda medida restrictiva debe ser *idónea (FJ 3ª), necesaria (FJ 5ª), y ponderada (FJ 5ª)*. La STC 66/1995 contiene estos subprincipios:

1) Idoneidad o juicio de adecuación: para adoptar una medida restrictiva de un derecho, ésta debe ser adecuada e idónea, es decir, apta para lograr la finalidad legítima prevista por la norma. El juicio de adecuación requiere por tanto un previo examen acerca de la legitimidad del fin perseguido por la norma y de la aptitud de esta para lograrla, de tal forma que la ley o medida restrictiva ha de mostrarse consistente con el bien o con la finalidad en cuya virtud se establece.

[162] Artículo 35 de la Ley 39/2015 , de 1 octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

[163] STC 66/1995, de 8 de mayo (Sala segunda), FJ 3º y FJ 5º.

2) Necesidad, imprescindibilidad o juicio de indispensabilidad: si la finalidad es legítima y la norma adecuada, se procede a analizar si la medida es la menos gravosa para la consecución del fin, identificando si existen otras menos lesivas. En otros términos, no debe existir otro medio igualmente eficaz y menos limitativo para conseguir los mismos resultados.
3) Proporcionalidad en sentido estricto: implica establecer un orden de preferencia relativo para el supuesto concreto, que puede variar en otro supuesto en atención a las concretas circunstancias presentes. Y tal orden se establece idealmente a través de tres fases sucesivas: en primer lugar, se identifican los principios (valores, bienes, intereses) en conflicto; en segundo lugar, se atribuye a cada uno de ellos la importancia que le corresponda, según las circunstancias del caso; y, por último, se otorga prevalencia a uno (o unos) sobre el otro (los otros)[164].

Estos tres subprincipios mencionados, más el del fin legítimo es lo que la dogmática jurídica entiende por el "test de la proporcionalidad" (también llamado "test alemán de proporcionalidad"), siendo unos criterios que permiten determinar la factibilidad de la ponderación en cada caso[165].

El principio de proporcionalidad también es exigido por el artículo 52 la Carta de los Derechos Fundamentales de la Unión Europea a la hora ordenar conflictos entre los derechos y/o principios en ella contenida y en este orden de cosas, no se puede dejar pasar por alto que el TJUE ha insistido que los requisitos de necesidad y proporcionalidad deber tenerse muy presentes a la hora regular o limitar un derecho fundamental[166].

El principio de proporcionalidad es pues, la figura jurídica en la que se sustentan las decisiones normativas y resolutivas ante las situaciones de emergencia. De acuerdo con el contenido de este documento, de aplicación a las medidas que implican usos de datos personales para la gestión de la pandemia de 2020.

Tal y como se señala en este documento más adelante, tanto el artículo 3 de la Ley orgánica 3/1986[167], como el artículo 54 de la Ley 33/2011[168], contienen en su redacción una cláusula muy abierta que permiten la adopción de "medidas necesarias", no tasadas, para afrontar una situación de emergencia que por definición se caracterizan por su imprevisibilidad. Es evidente que se hace referencia a la pandemia COIVD-19.

Estas determinaciones contenidas en la Ley conllevan que el aplicador de estos artículos, el Gobierno o la Administración, tendrán que adoptar medidas necesarias proporcionales[169] y motivadas de forma suficiente siguiendo las tres fases del

[164] RODRÍGUEZ DE SANTIAGO, JM. (2000), "La ponderación de bienes …..", op.cit; pp 121-138.
[165] BAQUERIZO MINUCHE, J. (2009) "Colisión de los Derechos …..", op.cit; p 18. p 36, 4º párrafo.
[166] STJUE de 8 de abril de 2014 (Gran Sala) (asuntos C-293/12 y C-594/12), apartado 61, p 20.
[167] Ley orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.
[168] Ley 33/2011, de 4 de octubre, General de Salud Pública.
[169] DE LA SIERRA, S., (2020), "Lectura de urgencia de las reacciones frente al COVID-19 desde la óptica jurídica internacional comparada". El Cronista del Estado Social y Democrático de Derecho, 86-86; 32-41 y MARTÍNEZ MARTÍNEZ, R., (2020) "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", Diario La Ley, 9601 (28/02/2021).

procedimiento de ponderación. En este contexto, ninguna medida puede considerarse a priori y per sé ilegal e inconstitucional, siempre claro está, en el caso del derecho a la protección de datos de carácter personal se respete las garantías mínimas contenidas en el RGPD y Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales.

El principio de proporcionalidad se opone a medidas restrictivas indefinidas. Este conocimiento preciso, en el caso de la situación creada por la COVID-19 ha de entenderse circunscrito al conocimiento posible, dado que no se puede obviar que tanto el juicio de idoneidad como el de necesariedad[170] se realizará en un contexto de *incertidumbre sanitaria y científica*. Se trata de un contexto de incertidumbre sanitaria y científica, por lo que entra en juego también el "principio de precaución"[171].

En este sentido, no sólo hay que seleccionar las categorías de datos relevantes y adecuadas para el problema que se ha de abordar, sino que hay que extraer datos que sean de calidad, fiables y contrastados. Ese subconjunto de datos interconectados que realmente tienen y aportan valor se denomina información. La recogida masiva e indiscriminada de datos personales no solo incumple con los principios de necesidad y proporcionalidad, sino que conduce a la agresión contra los derechos y libertades de los ciudadanos y el riesgo que dichos datos acaben en las manos equivocadas que, con un plan claro, recursos y decisión suficiente, vuelvan esos datos contra nosotros. El conocimiento es el que permite la toma de decisiones adecuadas[172]. El control, reducción y eliminación de riesgos en la protección de los datos de las personas es una constante en el RGPD, el artículo 23.1.g), entiende que hay que salvaguardar de los riesgos para los derechos y libertades de los interesados y el artículo 30 versa específicamente sobre los riesgos de las actividades de tratamientos, entre otros artículos.

2.4. El impacto de la regulación del derecho de la protección de datos en el procedimiento administrativo y en la organización administrativa.

Se puede afirmar que la regulación del derecho fundamental a la protección de datos de carácter personal ha tenido un impacto singular en las técnicas e instituciones clásicas

[170] VELASCO CABALLERO F., (2020) "Libertad, Covid-19 y proporcionalidad (I): fundamentos para un control de constitucionalidad". Blog independiente de Francisco Velasco. Disponible en: https://franciscovelascocaballeroblog.wordpress.com/2020/05/30/libertad-covid-19-y-proporcionalidad-i-fundamentos-para-un-control-de-constitucionalidad/ y "Libertad, Covid-19 y principio de proporcionalidad (II): indicadores para el control de constitucionalidad." Blog independiente de Francisco Velasco (Disponible en: https://franciscovelascocaballeroblog.wordpress.com/2020/05/31/libertad-covid-19-y-principio-de-proporcionalidad-ii-indicadores-para-el-control-de-constitucionalidad / (28/02/2021).

[171] ESTEVE PARDO, J. (2020), "La apelación a la ciencia en el Gobierno y gestión de la crisis COVID-19", Revista de Derecho Público: Teoría y Método,2, 35 a 50. (30/04/2021). p 41.

[172] Así se asevera en la nota publicada por la AEPD el 14 de abril de 2020 la AEPD sobre "Tratamientos de datos personales en situaciones de emergencia". Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/tratamientos-datos-personales-situaciones-emergencia (28/02/2021).

del Derecho Administrativo, así lo han señalado autores de reconocido prestigio como JEAN-BERNARD AUBY, a propósito del estudio de las Ciudades Inteligentes[173].

Más allá de la vinculación con determinados principios, la vertiente objetiva de los derechos fundamentales encuentra en la organización y procedimiento "un medio -posiblemente el único existente- para producir un resultado acorde con los derechos fundamentales y, con ello, asegurar eficazmente los derechos fundamentales en vista de la problemática moderna"[174].

Pero esta idea de organización y procedimiento se presenta como una dualidad de reglas diferenciadas, lo que nos lleva, inevitablemente, a plantear su estudio por separado.

A continuación, nos centraremos en el procedimiento. En las reglas relativas a la sucesión de actuaciones en el desarrollo de la actividad. Toda la actividad de tratamiento de datos consiste en una sucesión de actuaciones regladas que deben desempeñar los responsables y/o los encargados del tratamiento de tales datos. Con ello, se intenta asegurar que la toma de decisiones sobre el tratamiento se ajustará a la Ley y, además, que se encaminará hacia una situación de equilibrio en los intereses del responsable y/o encargado del tratamiento y el titular de los datos, lo que, nuevamente, nos conduce a una idea de justicia material. De esta forma, podemos afirmar que la adhesión a esa sucesión de actuaciones determinará que el tratamiento sea legal y, también, que sea justo.

Si queremos trazar un esquema del *iter* procedimental del tratamiento de datos, sería el siguiente: en primer lugar, se deben determinar los medios del tratamiento y se debe realizar una evaluación previa de riesgos; en segundo lugar, hay que concretar el fundamento de licitud del tratamiento, es decir determinar si existe base jurídica para dicho tratamiento, bajo alguno de los supuestos de los artículos 6 ó 9 del Reglamento (UE) 2016/679; seguidamente y en tercer lugar, hay que recoger los datos con unos fines determinados, explícitos y legítimos; en cuarto lugar, se deben registrar y almacenar los datos, para lo cual se crearán los correspondientes ficheros y se llevará a cabo un registro de actividad; después, en quinto lugar, se llevará a cabo el tratamiento en sí de los datos, entendiendo por tratamiento cualquier operación realizada sobre los datos o conjunto de datos, en aplicación de los de los principios y derechos, que a continuación se estudian pormenorizadamente, y, en última instancia, se deberá proceder a la destrucción de los datos, ya sea mediante borrado, ya mediante bloqueo.

[173] AUBY, J.-B., (2018) "Algorithmes et Smart Cities: Données Juridiques", Revue Générale du Droit, 2018, pp. 3-4 ; 15-18 ; Contrôle de la puissance publique et gouvernance par algorithme, Galetta, D-U y Jacques Ziller, J. (Ed.) Le droit public au défi des technologies de l'information et de la communication, au-delà de la protection des donnés, Nomos. pp 153 –166.

[174] HESSE, K (1978) "Bestand und Bedeutung .....", op.cit; p 434.

Capítulo 3. Los principios de la protección y del tratamiento de datos en la normativa de protección de datos personales

3.1. Los principios de la protección y del tratamiento de datos en la normativa de protección de datos personales con carácter general

La cuestión jurídica de los principios requiere una cierta profundización y con más motivo se está refiriendo a una ley que protege un derecho fundamental. En este orden de cosas, este capítulo 3 del Título I, trata los principios de una forma breve e introductoria, dado que los principios se van tratando a lo largo de los Títulos I, II y III.

Los principios de la protección y del tratamiento de datos en la normativa de datos personales relativos a la salud de las personas, se analizan y comentan en el capítulo 2.1 del Título III, el cual se refiere al sector sanitario exclusivamente.

Los principios de las leyes son valores sobre los que se asienta la ley en su conjunto, afectan a todas sus directrices, derechos, obligaciones y a las interpretaciones que la realidad haga necesarias. Los principios de las leyes tienen un valor excepcional, pues inspiran al ordenamiento jurídico y lo impregnan en su conjunto. El principio que proclama una ley es extensible a todo el ordenamiento jurídico.

El Capítulo II, sobre principios, del Reglamento (UE) 2016/679, contiene desde el artículo 5 hasta el artículo 11. En la Ley Orgánica 3/2018, es el Título II sobre principios de protección de los datos, el que contiene del artículo 4 al artículo 10.

El primer principio que emana del Reglamento 2016/679 es el principio de proactividad, (en inglés, *accountability principle*), o responsabilidad proactiva que hace referencia concretamente a la proactividad de los responsables y encargados del tratamiento. Se trata de que estos no tan solo de cumplan el Reglamento (UE) 2016/679 sino que sobre todo puedan demostrarlo[175]:

> "El RGPD ha supuesto un cambio muy importante en el modelo de cumplimiento de la normativa de protección de datos porque se pasa de un modelo reglado, que establecía los requisitos que debían observarse, a un modelo en el que cada responsable del tratamiento de datos tiene que ser actuar de forma diligente, proactiva, analizar su situación, ver qué medidas tiene que adoptar en cada caso, e ir actualizando las medidas de cumplimiento. El RGPD ofrece flexibilidad a la hora de su cumplimiento, pero siempre bajo este principio que obliga no sólo a cumplir sino a poder demostrarlo".

La Agencia Española de Protección de Datos (AEPD) asigna este tipo de responsabilidad en la figura del responsable del tratamiento, dice en relación a este principio[176]:

[175] ESPAÑA M. (2019) "Entrevista en Revista Registradores de España". Revista del Consejo General de Colegios de Administradores de Fincas -CGCAFE-, 84 ,20-23 https://afcolegiadosblog.com/2019/07/30/entrevista-mar-espana-directora-de-la-agencia-espanola-de-proteccion-de-datos/ (28/02/2021).

[176] AEPD (2019) "Guía del Reglamento General de Protección de Datos. Para responsables del tratamiento". Guía de protección de datos UE. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf (31/01/2021). p 3.

> "El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo".

En este orden de cosas cabe destacar:

a. El preámbulo de la Ley Orgánica 3/2018, dice: "Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa".
b. El Reglamento (UE) 2016/679 determina que en responsable realizará la "Evaluación de impacto relativa a la protección de datos", artículo 35.
c. El principio de proactividad o de responsabilidad activa viene concretado en la Ley Orgánica 3/2018, a través del Capítulo I del Título V, sobre "Medidas de responsabilidad activa".

Otro principio que emana del Reglamento 2016/679 es el de la protección pasiva del dato, es decir, que la simple proclamación del propio Reglamento protege a todos los datos personales, todos los datos personales están protegidos recayendo la carga de la prueba en quién los trata y no en el titular de estos. En otras palabras, el Reglamento 2016/679 "no permite ningún tratamiento de ningún dato, prohibiendo además el tratamiento de determinados datos". Este extremo se deduce del artículo 6 (Licitud del Tratamiento). Este artículo dice en su punto 1.: "El tratamiento solo será lítico si cumple al menos una de las siguientes condiciones", añadiendo un listado de 6 condiciones bajo las cuales el tratamiento se considera legal. En consecuencia, todo tratamiento que no pueda incluirse en este listado se entenderá como un tratamiento no licito o ilícito y, por otra parte, la sola necesidad de datos personales para un propósito no justifica llevar a cabo cualquier tipo de tratamiento y con cualquier frecuencia[177].

Otro principio del Reglamento (UE) 2016/679 es el principio de minimización de los datos personales que aparece en el artículo 5, sobre Principios relativos al tratamiento, artículo 25, sobre Protección de datos desde el diseño y por defecto, artículo 47, sobre Normas corporativas vinculantes, artículo 89, sobre Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos del Reglamento, y Considerando 156 del Reglamento (UE)

[177] AEPD (2020) "Guía de protección de datos por defecto". Octubre 2020. Disponible en https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf (31/01/2021). p 12.

2016/679. No es posible, pues, recabar y tratar datos solo por si pudiera ser necesario en un futuro[178].

La nueva legislación además de no legitimar cualquier tratamiento sino solo los del numerus clausus del artículo 6 además prohíbe el tratamiento de determinados datos, en concreto incluye los datos de salud, tal como aparece en el artículo 9, sobre Tratamiento de categorías especiales de datos personales, del Reglamento 2016/679.

Por otra parte, también es cierto que en el apartado 2 del mismo artículo 9, se dice que no se aplicará el punto 1 del artículo 9 en los supuestos que determina el Reglamento (UE), permitiendo utilizar los datos de las categorías especiales en determinados supuestos sin la autorización del interesado, es decir, sin su consentimiento.

A todo ello, el binomio Reglamento 2016/679 y Ley Orgánica 3 / 2018 relativo a la protección del dato lo que realmente hace es regular el tratamiento de los datos limitando de forma importante todo lo relacionado con el mismo, así pues, no es pérdida de tiempo acudir a la norma para concretar lo que la legislación entiende por los principios que rigen en el tratamiento de los datos personales.

Tabla 2. Principios del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018 (elaboración propia)

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales					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				
Título	II			Principios de protección de datos	Capítulo	II			Principios
		Artículo	4	Excatitud de los datos					
		Artículo	5	Deber de confidencialidad			Artículo	5	Principios relativos al tratamiento
		Artículo	6	Tratamiento basado en el consentimiento del afectado			Artículo	6	Licitud del Tratamiento
							Artículo	7	Condiciones para el consentimiento
		Artículo	7	Consentimiento de los menores de edad			Artículo	8	Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información
		Artículo	8	Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos					
		Artículo	9	Categorías especiales de datos			Artículo	9	Tratamiento de categorías especiales de datos personales
		Artículo	10	Tratamiento de datos de naturaleza penal			Artículo	10	Tratamiento de datos personales relativos a condenas e infracciones penales
							Artículo	11	Tratamiento que no requiere identificación

Los principios que aparecen en el Capítulo II del Reglamento (UE) y en el Título II de la Ley Orgánica (Tabla 2) son los siguientes:

A) La licitud, la lealtad y la transparencia, con relación al interesado: aparece en el artículo 5.1.a de Reglamento (UE) 2016/679. La licitud del tratamiento se

[178] INAP (2020) "Curso de Reglamento General de Protección de Datos". Instituto Nacional de Administración pública Disponible en https://www3.gobiernodecanarias.org/cpji/ gestionconocimiento /_recursos/97rotección_datos/resources/Modulo_1.pdf (28/02/2021). P 13.

desarrolla en el artículo 6 de Reglamento (UE) 2016/679[179]. La licitud tendrá que serlo en cuanto al tratamiento y a la finalidad, pero también atendiendo a los medios (STS 2484/2019, FD 3º)[180].

B) La limitación de la finalidad: los datos no serán tratados con fines distintos por los que fueron recogidos. Aparece en el artículo 5.1.b de Reglamento (UE) 2016/679. En este sentido la AEPD aclara esta expresión y en la Guía para el Ciudadano[181] se dirige a este diciendo:

> "Tus datos personales serán recogidos para unos fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con otros fines. Ejemplo: Si recaban tus datos personales y te informan que "son tratados para mejor tu experiencia como usuario", esta finalidad no se ajustaría a este principio."

C) La minimización de datos: adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, en este orden de cosas, no se recabaran datos sin un fin determinado. Aparece en el artículo 5.1.c de Reglamento (UE) 2016/679. La importancia y relevancia de este principio es el que justifica la elaboración de la Guía de la Protección de Datos por Defecto editada por la AEPD en otubre de 2020[182] y que a su vez viene justificada:

> "Esta guía desarrolla de forma práctica la aplicación de la protección de datos por defecto, o PDpD, en los tratamientos de datos personales a partir de lo establecido en el artículo 25 del RGPD y la guía publicada por el Comité Europeo de Protección de Datos "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"."

En este orden de cosas la AEPD entiende que el principio de minimización reflejado en el RDPG en su artículo 5.1.c) es de tal importancia que debe aplicarse ya en el diseño del tratamiento futuro de los datos que se pretendan tratar, de esta forma:

> "Las medidas de PDpD giran en torno a la aplicación racional del principio de minimización de datos, bajo los criterios de adecuación, pertinencia y necesidad con relación a los fines en el diseño de las distintas fases del tratamiento, tal como establece el artículo 25.2."

Este principio es para algunos autores la antítesis del big-data dado que de la lectura del RGPD cabe inferir que el principio de minimización impide una acumulación

[179] El Abogado de Estado de esta forma lo hace constar en el Quinto Antecedente de Hecho, p 8, al decir "Cualquier conocimiento de los datos personales por el OS tiene su fundamento y licitud en el artículo 6 del Reglamento 2016/679, como luego se examina". STS 2484/2019 de 12 de julio (Sala de lo Contencioso).

[180] STS 2484/2019 de 12 de julio (Sala de lo Contencioso), FD 3º.

[181] AEPD (2019) "Protección de Datos: Guía para el Ciudadano". Octubre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf (28/02/2021).

[182] AEPD (2020) "Guía de protección de datos por defecto". Octubre 2020. Disponible en https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf (31/01/2021).

masiva e indiscriminada de datos de salud sean o no pertinentes para el fin perseguido[183].

D) La exactitud de los datos: este principio es nombrado como tal en la Ley Orgánica 3/2018, artículo 5, e incluido dentro de los principios relativos al tratamiento en el Reglamento (UE) 2016/679, artículo 5. No tan solo exactos sino actualizados[184], explicando que "De gran cantidad de tratamientos de datos se derivan decisiones que pueden afectar, en ocasiones de forma significativa, a los derechos o intereses de los titulares de datos". De esta forma, los datos deberán ser exactos y para ellos deberán estar actualizados, suprimiendo o rectificando, sin dilación, los datos personales inexactos en base a los fines de su tratamiento[185].

   La AEPD edita en el año 2020, concretamente en febrero el documento "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción"[186], en este documento la Agencia dedica el apartado D) al concepto de exactitud de los datos, concretamente en el entorno de la inteligencia artificial enumera lo factores que influyen en la exactitud.

E) La confidencialidad: el deber de confidencialidad es un principio nombrado como tal en la Ley Orgánica 3/2018, artículo 6, e incluido dentro de los principios relativos al tratamiento en el Reglamento (UE) 2016/679, artículo 5. La AEPD, en la Resolución de 2 de julio de 2019[187] define el alcance del criterio de confidencialidad en este ámbito:

   > "Integridad y confidencialidad: los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido aquél;"

F) Licitud de tratamiento: este principio es proclamado explícitamente por el Reglamento (UE), artículo 6, y no aparece en la Ley Orgánica. Este principio tiene una extrema importancia, a tenor literal dice: "El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones", lo que se desprende que para

[183] BELTRÁN AGUIRRE, JL (2018) "Reglamento general de protección de datos: novedades. Adaptación de la normativa española: El proyecto de LOPD". Revista Derecho y Salud, 28 (1), p 74-76. P 85.

[184] AEPD (2019) "Protección de Datos: Guía para el Ciudadano". Octubre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf (28/02/2021).

[185] STJUE de 24 de septiembre de 1989 (Gran Sala) asunto C-136/7 apartado 16.d). p 7.

[186] AEPD (2020) "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción". Febrero 2020. Disponible en https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (31/01/2021).

[187] AEPD (2019) Resolución de 2 de julio de 2019 de la Directora de la Agencia Española de Protección de datos, Autoridad Administrativa Independiente (AEPD), por la que se aprueba la Política de protección de datos y seguridad de la información de la AEPD y se derogan las resoluciones de la Directora de la Agencia de 10 de mayo de 2018, por la que se aprueba la Política de protección de datos y seguridad de la información de la Agencia Española de Protección de datos, y la resolución de 15 de junio de 2016, por la que se aprueba la política de seguridad de la información de la AEPD.

el Reglamento (UE) el tratamiento de datos no está autorizado por la ley y que tan solo se considerará licito en el caso de cumplir el listado de supuestos de licitud expresados en el artículo 6. El TJUE entiende por licitud del tratamiento cuando este es proporcional y necesario[188].

G) El consentimiento: concretamente la Ley Orgánica se refiere al principio del tratamiento basado en el consentimiento del afectado, artículo 6, mientras que el Reglamento de la (UE) incluye el consentimiento como un criterio de licitud. Sin embargo, el Reglamento (UE) dedica el artículo 7 a lo que denomina Condiciones del Consentimiento, recayendo la carga de la prueba del consentimiento en el responsable del tratamiento. El consentimiento debe ser dado libremente, artículo 7.4 Reglamento (UE), y la mera información al interesado del tratamiento de sus datos no puede ser entendida en absoluto como un trámite dentro del consentimiento[189]. La información para el consentimiento debe incluir de forma clara y precisa las finalidades del tratamiento[190]. Además, el Tribunal Supremo en 2020 entiende que "la utilización sin consentimiento de los datos personales constituye una infracción individualizada, con independencia de que esa utilización o tratamiento de datos"[191].

H) El consentimiento del menor: aparece diferenciada en las dos normas. En el Reglamento (UE) se dedica el artículo 8, mientras la Ley Orgánica le dedica el artículo 7. El Reglamento sitúa la edad mínima del menor en 16 años, mientras que la Ley Orgánica en 14 años. La AEPD en el mes de diciembre de 2020 editó una guía para protección de datos en menores de 18 años y la cuestión del consentimiento[192], de esta forma:

> "En menores de 14 años.
>
> El consentimiento para la utilización de sus datos personales se otorgará por sus padres o tutores legales. Art. 7.1 LOPDGDD.
>
> El responsable del tratamiento hará esfuerzos razonables para verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible. Art. 8.2 RGPD.
>
> En menores entre 14 y 18 años.
>
> Podrán otorgar el consentimiento para la utilización de sus datos personales por sí mismos, salvo que una norma específica exija la asistencia de los padres o tutores. Art. 7.1 LOPDGDD."

[188] STJUE de 16 de diciembre de 2008 (Gran sala) (asunto C-524/06) apartado 52.

[189] STJUE de 9 de noviembre de 2010 (Gran sala) (asuntos C-92/09 y C-93/09), apartado 64, p I-11147.

[190] AEPD (2018) Resolución de la Agencia Española de Protección de Datos R/00259/2018, de 2 de marzo de 2018.

[191] STC 3891/2020 de 19 de noviembre (Sala de lo Contencioso) FD 3º.

[192] AEPD (2020) "Información sobre consentimiento para tratar datos personales de menores de edad". Diciembre de 2020. Disponible en https://www.aepd.es/sites/default/files/2020-12/infografia-consentimiento- menores.pdf (31/01/2021).

A esta aclaración de la AEPD con relación al consentimiento de menores de 18 y de 14 años se añade el artículo 92 de la Ley Orgánica 3/2018, en relación a los responsables de los centros educativos:

> "Los centros educativos y cualesquiera otros que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información. Art. 92 LOPDGDD."

I) Las categorías especiales de datos: aparecen en ambos textos como principios. En la Ley Orgánica el artículo 9 se dedica a Categorías especiales de datos, mientras el Reglamento (EU) dedica el artículo 9 al tratamiento de las Categorías especiales de datos. A esta categoría especial de datos personales se conocen como datos sensibles, se prevé para ellos una seguridad reforzada[193].

J) El tratamiento de los datos de naturaleza penal, aparecen en los dos textos. El Reglamento (UE) dedica el artículo 10 al tratamiento de datos personales relativos a condenas e infracciones penales, mientras la Ley Orgánica dedica el artículo 10 al Tratamiento de datos de naturaleza penal.

K) El tratamiento de los datos sin identificación: el Reglamento (UE) dedica el artículo 11 al Tratamiento de datos que no requieren identificación. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

L) Otros principios: el Reglamento (UE) 2016/679 añade una serie de principios distintos de los mencionados con anterioridad de esta forma se refiere al principio de periodos de conservación limitados; al de la calidad de los datos; al de la protección de los datos desde el diseño y por defecto; al de la base del tratamiento; y al principio de las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes, artículo 47, Normas corporativas vinculantes, Reglamento (EU) 2016/679.

Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable, no a la anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación, tal como consta en el Considerando 26 del Reglamento (UE) 2016/679.

[193] SAN 4845/2018 de 20 de diciembre (Sala de lo Contencioso), FD 6º.

Capítulo 4. Los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de los datos personales

4.1. Introducción a los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de los datos personales

Este capítulo trata sobre los derechos que permiten la aplicación del derecho fundamental de la protección de datos, es un capítulo que analiza los medios que dispone el Reglamento y la Ley para que el ciudadano pueda exigir su efectividad. En este orden de cosas, este capítulo 4 del Título I, describe los derechos del cuidando dirigidos a su protección en cuanto a sus datos se refiere, de una forma breve e introductoria, dado que los derechos se van tratando a lo largo de los Títulos I, II y III.

Los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de los datos personales relativos a la salud, se analizan y comentan en el capítulo 2.2 del Título III, el cual se refiere al sector sanitario exclusivamente.

Tanto el Reglamento (UE) 2016/679 como la Ley Orgánica 3 /2018 crean y proclaman unos derechos para los ciudadanos. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario. Sin embargo, es realmente el Reglamento (EU) 2016/679 el que define y por tanto crea tales derechos, tal como se desprende de la lectura de los artículos 11 al 18 de la Ley Orgánica 3/2018, la cual se remite reiteradamente a lo dispuesto en el Reglamento (UE) 2016/679.

En virtud del Reglamento (UE) 2016/679, de 27 de abril, Reglamento Europeo de Protección de Datos, aplicable desde el 25 de mayo de 2018, a los tradicionales derechos de acceso, rectificación, cancelación y oposición, se suman otros nuevos: de olvido, de portabilidad de los datos, a la limitación del tratamiento y a no ser objeto de decisiones individualizadas. Este último pretende evitar ser víctima o producto de una decisión basada únicamente en el tratamiento de tus datos, la elaboración de perfiles, que produzca efectos jurídicos sobre la persona[194].

Previo al artículo 15, sobre los derechos de acceso, el Reglamento (UE) en su artículo 1 manifiesta que establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. Por tanto, el primer derecho que protege es el de la protección de las personas físicas en lo que se refiere a los datos personales.

Seguidamente el artículo 1 del Reglamento (UE) manifiesta que protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. “El derecho de protección de datos personales ha

[194] AEPD (2019) Sede electrónica de 20 de julio de 2019. “Derecho a no ser objeto de decisiones individuales automatizadas”. Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-no-ser-objeto-de-decisiones-individuales (28/02/2021).

surgido después de un cambio jurídico radical acaecido en esta materia en los últimos dos siglos y medio."[195]

Por último, el artículo 1, ratifica uno de los derechos fundamentales de la Unión Europea, el derecho de la libre circulación de los datos personales en la Unión que no podrá ser restringido ni prohibido por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. En consecuencia, el Reglamento (UE) defiende el derecho a la libre circulación, tan solo que atendiendo a una serie de cautelas y reglas que el propio Reglamento (UE) específica y desarrolla.

Reglamento (UE) 2016/679 reconoce como un derecho la transparencia e información al interesado, el derecho de acceso en el sentido de que el titular tendrá derecho de obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales suyos y en dicho caso, tener derecho al acceso a estos, el derecho de rectificación sobre los datos inexactos que conciernan personalmente que deberá realizar el responsable del tratamiento, el derecho de supresión sin dilación mediante la eliminación de sus datos, el derecho a la limitación del tratamiento, el derecho a la portabilidad en cuanto debe poder recibir sus datos personales en soporte común y por último, el derecho de oposición en cuanto el sujeto puede negarse a que sus datos sean tratados o sometidos a determinados tratamientos.

En cuanto a la Ley Orgánica 3/2018, el objeto de la Ley es adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones sin contravenirlo. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta Ley Orgánica. A este objetivo se añade otro, garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

La AEPD publicó un documento en internet el día 20 de julio de 2019 con el título "Ejerce tus derechos"[196] en el cual explica que "La normativa de protección de datos permite que puedas ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas".

[195] PASCUAL HUERTA, P. (2017) "La génesis del derecho fundamental a la protección de datos Personales", Tesis Doctoral, Facultad de Derecho, Universidad Complutense de Madrid. Madrid. España. p 290.

[196] AEPD (2019) "Ejerce tus derechos". 20 de Julio de 2019. Disponible en https://www.aepd.es/ es/ derechos-y-deberes/conoce-tus-derechos (31/01/2021).

Tabla 3. Los derechos en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018 (elaboración propia)

Los derechos que reconocen el nuevo ordenamiento jurídico de protección de datos (Anexo D)

Derechos		Derechos	
	Reglamento (UE) 2016/7679	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	
Cap. III	Derechos del interesado	Derechos de las personas	Título III
		Transparencia e información	Cap. I
Sección 1	Transparencia y modalidades		
Art. 12	Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado	Transparencia e información al afectado	Art.11
		Ejercicio de los derechos	Cap. II
Sección 2	Información y acceso a los datos personales		
		Disposiciones generales sobre ejercicio de los derechos	Art. 12
Art. 13	Información que deberá facilitarse cuando los datos personales se obtengan del interesado		
Art. 14	Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado		
Art.15	Derecho de acceso del interesado	Derecho de acceso	Art, 13
Sección 3	Rectificación y supresión		
Art. 16	Derecho de rectificación	Derecho de rectificación	Art. 14
Art.17	Derecho de supresión («el derecho al olvido»)	Derecho de supresión	Art. 15
Art.18	Derecho a la limitación del tratamiento	Derecho a la limitación del tratamiento	Art.16
Art.19	Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento		
Art. 20	Derecho a la portabilidad de los datos	Derecho a la portabilidad	Art.17
Sección 4	Derecho de oposición y decisiones individuales automatizadas		
Art. 21	Derecho de oposición	Derecho de oposición	Art. 18
Art. 22	Decisiones individuales automatizadas, incluida la elaboración de perfiles		

El documento "Ejerce tus derechos"[197] de la AEPD de 2019, enumera las siguientes nueve (9) características de estos derechos:

1. "Su ejercicio es gratuito
2. Si las solicitudes son manifiestamente infundadas o excesivas (p. ej., carácter repetitivo) el responsable podrá:
    - cobrar un canon proporcional a los costes administrativos soportados
    - negarse a actuar
3. Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más
4. El responsable está obligado a informarte sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio

[197] AEPD (2019) "Ejerce tus derechos". 20 de Julio de 2019. Disposición en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos (31/01/2021).

5. Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo
6. Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una autoridad de control
7. Puedes ejercer los derechos directamente o por medio de tu representante legal o voluntario
8. Cabe la posibilidad de que el encargado sea quien atienda tu solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule
9. Si bien en las páginas siguientes de detallan todos los derechos y la forma con que cada norma los trata, el resumen de los derechos son los que constan en la Tabla 3."

Los derechos reconocidos en el Capítulo III del Reglamento (UE) 2016/679 y el Título III de la Ley Orgánica 3/2018:

A) La transparencia e información al afectado: recogido por el artículo 12 del Reglamento (UE) y por el artículo 11 de la Ley Orgánica. Este derecho distingue el hecho de que los datos hayan sido obtenidos del afectado o cuando han sido obtenidos por otras vías. El responsable del tratamiento deberá informar al afectado de la identidad del responsable del tratamiento, la finalidad del tratamiento y la posibilidad de ejercer los derechos de acceso, rectificación, supresión, imitación de tratamiento, portabilidad, oposición y la no elaboración de perfiles. En el supuesto de que los datos hubieran sido obtenidos por otras vías, se deberá informar al afectado las fuentes y categoría de los datos[198].

B) El derecho de acceso: recogido en el artículo 15 del Reglamento (UE) y por el artículo 13 de la Ley Orgánica. Cualquier persona tiene derecho a exigir del responsable de un tratamiento de datos la confirmación sobre si se están tratando datos personales de su titularidad. Se entenderá otorgado el derecho cuando el afectado tenga acceso remoto directo y seguro a la totalidad de sus datos, permanentemente. En cualquier caso, el afectado tendrá derecho al acceso a sus datos personales, a obtener una copia de ellos y a conocer:

    1. "la identidad y los datos de contacto del responsable y, en su caso, de su representante
    2. los datos de contacto del delegado de protección de datos, en su caso
    3. los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento
    4. los intereses legítimos del responsable o de un tercero;
    5. los destinatarios o las categorías de destinatarios de los datos personales
    6. en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional"

[198] AEPD (2019) "Guía para el cumplimiento del deber de informar". Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf (28/02/2021).

Este derecho tiene una importancia especial, pues tal como afirma el TJUE, resulta indispensable para que el interesado pueda ejercer los derechos de rectificación, supresión, bloqueo y la notificación a los terceros de toda rectificación, supresión o bloqueo de datos[199].

C) El derecho a la rectificación: recogido por el artículo 16 del Reglamento (UE) y por el artículo 14 de la Ley Orgánica. El interesado tendrá derecho a obtener del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional. Todo ello sin dilación indebida. La AEPD facilita a través de su página web el formulario[200] (Anexo [E]).

D) El derecho a la supresión: llamado también "derecho al olvido"[201] está recogido por el artículo 17 del Reglamento (UE) y por el artículo 15 de la Ley Orgánica. Este derecho está muy vinculado con los motores de búsqueda utilizados en Internet, tal como desvela la STJUE en el caso Google de 2014[202]. Además, en base a este derecho el interesado tendrá derecho a obtener del responsable del tratamiento la supresión o eliminación de los datos personales inexactos, sin dilación indebida, en los supuestos siguientes:

1. "los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo
2. el interesado retire el consentimiento en que se basa el tratamiento
3. el interesado se oponga al tratamiento
4. los datos personales hayan sido tratados ilícitamente;
5. los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento
6. los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8 del Reglamento (UE) sobre condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información"

El Tribunal Supremo en su Sentencia de 27 de noviembre de 2020 realiza un importante recopilación legislativa y jurisprudencial en su segundo fundamento jurídico que viene a denominar "Sobre el marco normativo aplicable y acerca de la doctrina jurisprudencial que resulta relevante para resolver el recurso de

[199] STJUE de 7 de mayo de 2009 (Sala tercera) (asunto C-553/07) apartado 49-52.

[200] AEPD (2019) Sede electrónica de 20 de julio de 2019. "Derecho de rectificación". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-rectificacion (28/02/2021).

[201] AEPD (2019) Sede electrónica de 20 de julio de 2019. "Derecho de supresión ("al olvido")" Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-supresion-al-olvido (28/02/2021).

[202] STJUE de 13 de mayo de 2014 (Gran sala) (asunto C-131/12), apartado 17. pp 7-8.

casación" y que introduce diciendo: "procede reseñar el marco jurídico aplicable así como la doctrina del Tribunal Constitucional y la jurisprudencia del Tribunal de Justicia de la Unión Europea formuladas sobre la naturaleza, el alcance, el significado, el contenido y los límites del derecho al olvido". La Sentencia ponderando dos intereses en conflicto, el derecho a la información frente al derecho al olvido, concluye que el derecho al olvido no es ilimitado y que en el entorno de la información personal publicada en internet ofrecida por los buscadores se debe al marco del menoscabo del derecho al honor, a la intimidad, o a la propia imagen del interesado, y carezca de interés público, y pueda considerarse, por el transcurso del tiempo, obsoleta[203].

E) El derecho a la limitación del tratamiento: recogido por el artículo 18 del Reglamento (UE) y por el artículo 16 de la Ley Orgánica. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación al tratamiento de sus datos de los datos en los siguientes supuestos:

1. "el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos
2. el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso
3. el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones
4. el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado"

La AEPD facilita a través de su página web el formulario[204] (Anexo [F]).

F) El derecho a la portabilidad: recogido por el artículo 20 del Reglamento (UE) y por el artículo 17 de la Ley Orgánica. No obstante, este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el

[203] "El ejercicio del derecho de oposición, rectificación o cancelación del tratamiento de datos, y, en su caso, del derecho al olvido, reconocido en el artículo 6.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con lo dispuesto en el artículo 18 del citado texto legal, en consonancia con lo dispuesto en los artículos 12 y 14 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, faculta a la persona interesada a exigir del gestor de un motor de búsqueda que elimine de la lista de resultados, obtenida como consecuencia de una búsqueda efectuada tanto a partir de su nombre completo o de sus dos apellidos, vínculos a páginas webs, publicados legalmente por terceros, que contengan datos e informaciones veraces, relativos a su persona, cuando la difusión de dicha información, relativa a su persona, menoscabe el derecho al honor, a la intimidad, o a la propia imagen del interesado, y carezca de interés público, y pueda considerarse, por el transcurso del tiempo, obsoleta, en los términos establecidos por la jurisprudencia del Tribunal de Justicia de la Unión Europea, del Tribunal Constitucional y del Tribunal Supremo." STS 4016/2020 de 27 de noviembre de 2020 (Sala de los Contencioso).FD 4º.

[204] AEPD (2019) Sede Electrónica de 20 de julio de 2919. "Derecho a la limitación del tratamiento". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-limitacion-del-tratamiento (28/02/2021).

cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable[205]. El interesado tendrá derecho a obtener y recibir del responsable del tratamiento los datos personales, mediante un formato de uso común y lectura mecánica, cuando:

1. El tratamiento este basado en el consentimiento
2. El tratamiento se realice por medios automatizados

La AEPD facilita a través de su página web el formulario[206] (Anexo [G]).

G) El derecho de oposición: recogido por el artículo 21 del Reglamento (UE) y por el artículo 18 de la Ley Orgánica. El interesado tendrá derecho a oponerse a que sus datos sean tratados, salvo que el responsable del tratamiento acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. Esta salvedad no se aplica en tratamientos de mercadotécnica. El ejercicio de oposición implica el cese del tratamiento de los datos. La AEPD facilita a través de su página web el formulario[207] (Anexo [H]).

Con carácter general, cabe decir que la prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable y que el responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

En relación con los derechos del menor, en cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de quince años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de la Ley Orgánica 3/2018.

[205] AEPD (2019) Sede Electrónica de 20 de julio de 2919. “Derecho a la portabilidad”. Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-portabilidad (28/02/2021).

[206] AEPD (2019) Sede Electrónica de 20 de julio de 2919. “Derecho a la portabilidad”. Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-portabilidad (28/02/2021).

[207] AEPD (2019) Sede Electrónica de 20 de julio de 2919. “Derecho a oposición”. Disponible en https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-oposicion.pdf (28/02/2021).

Los datos sometidos a tratamiento podrán haber sido obtenidos del interesado o no obtenidos del interesado, tal circunstancia hará que el afectado reciba además de la información básica, es decir, la identidad del responsable del tratamiento y de su representante, en su caso, la finalidad del tratamiento y a la posibilidad de ejercer los derechos, se suministrarán las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos, artículos 15 al 22 del Reglamento (UE) 2016/679.

El titular deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

Además, el Reglamento (UE) 2016/679 reconoce los siguientes derechos:

a. Derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, artículo 77 del Reglamento (UE) 2016/679.
b. El derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento. Todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales, artículo 79 del Reglamento (UE) 2016/679.
c. Representación de los interesados. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro, artículo 80 del Reglamento (UE) 2016/679.
d. Derecho a indemnización y responsabilidad. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del Reglamento (UE) 2016/679 tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos, Artículo 82 del Reglamento (UE) 2016/679.

Capítulo 5. Tratamiento de los datos en base a la norma de protección

5.1. Tratamiento de datos en general

El Reglamento (UE) 2016/679 en su primera consideración reconoce que la protección de los datos de las personas físicas corresponde a un derecho fundamental de las mismas, dice:

> "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan."

En su consideración cuarta, el Reglamento (UE) 2016/679, añade unos límites razonables a este derecho por entender que el derecho a la protección de los datos personales no es un derecho absoluto. Estos límites nacen del principio de proporcionalidad y se aplican a otros derechos fundamentales de las personas y libertades de la Carta conforme a los Tratados.

De esta forma, si bien la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales se refiere al concepto de protección de datos personales, el Reglamento (UE) 2016/679 concreta más y se hace denominar "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", es decir, de lo que trata es de controlar y regular el tratamiento de los datos de las personas físicas, pero no tan solo para la protección del derecho y libertades fundamentales de las personas física sino también para proteger la libre circulación de personas físicas y la de sus datos.

A su vez, el reglamento determina que no es posible cualquier tratamiento de datos personales, sino tan solo cuando este sea lítico. Es decir, el Reglamento (UE) protege a las personas físicas regulando el tratamiento de sus datos personales, de todos ellos, en un determinado ámbito material, artículo 2 del Reglamento, a través de unos principios comunes a todo tratamiento, artículo 5, incluyendo tanto al dato como al responsable de su tratamiento y definiendo en qué casos es lícita esta actividad humana.

En este orden de cosas, no está permitido el tratamiento de datos personales, exceptuando los generados en los supuestos del artículo 2.2 del Reglamento (UE) 2016/679, salvo que estos estén legitimados por los supuestos del artículo 6.1 y no estén prohibidos por el artículo 9. Así pues, el ordenamiento jurídico de la Unión Europea al exigir licitud en el tratamiento de los datos personales, está diciendo que tratarlos no es lícito, prohibiendo expresamente el tratamiento de determinados datos llamados datos de categorías especiales, salvo circunstancias especiales determinadas en el artículo 9.2 del Reglamento.

El tratamiento de datos personales sólo tiene base jurídica cuando se cumple alguno de los supuestos recogidos en el artículo 6 del Reglamento y las otras diez condiciones del

artículo 9 en los tratamientos prohibidos, en consecuencia, habrá que demostrar la licitud en el procedimiento.

Las condiciones de licitud mencionadas se resumen en las siguientes ideas: por el consentimiento del interesado libre, claro y explicito; por exigencias del acto jurídico (contratos) de su interés; por algún tipo de obligación legal (del responsable del tratamiento); por la protección de intereses vitales, por interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; cuando haya que satisfacer 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[208].

En base al artículo 9 se regulan los tratamientos prohibidos. En este orden de cosas, está explícitamente prohibido el tratamiento de datos personales cuando estos revelen ciertas características de las personas protegidas por las leyes o que su discriminación sea ilegal o que no se puedan tener en consideración para distinguir tratos o derechos entre las personas.

Estas características o elementos se recogen en el siguiente listado: el origen étnico o racial; las opiniones políticas; las convicciones religiosas o filosóficas; la afiliación sindical; el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física; datos relativos a la salud o datos relativos a la vida sexual; o las orientaciones sexuales de una persona física.

Esta prohibición deja de serlo cuando existe base jurídica, que ocurre cuando el interesado hubiera hechos públicos sus datos o se dan una de estas circunstancias cuando medie consentimiento explícito y libre del interesado en base al artículo 7 del Reglamento (UE) 2016/779 y siempre que este consentimiento no esté legalmente prohibido.

Ahora bien, no se requerirá consentimiento para el tratamiento de datos cuando dicho tratamiento tenga como fin el cumplimiento legal de obligaciones, del responsable del tratamiento o del interesado, en el ámbito del Derecho laboral y de la seguridad y protección social o cuando el fin sea el ejercicio legal de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social. Tampoco será preciso el consentimiento del interesado, en el caso incapacidades o incapacitaciones físicas o jurídicas para emitir consentimiento, cuando se deba proteger cualquier interés vital, del interesado o de otra persona física.

A estas circunstancias eximentes de prohibición se deben añadir otras cuando dicho tratamiento se de en el ámbito de las actividades lícitas de una fundación, asociación o de cualquier otro organismo sin ánimo de lucro, con fines políticos, filosóficos, religiosos

[208] GUASCH PORTAS, V (2015) "El interés legítimo en la protección de datos". Revista de Derecho UNED, 16, 417-438. p 431.

o sindicales, el tratamiento de datos de los miembros actuales o antiguos de estas organizaciones o personas que se relacionen con las mismas. Cuando estos tratamientos de datos impliquen la comunicación fuera de dichas organizaciones, no se aplicar dicha eximente de prohibición.

También se levanta la prohibición cuando el tratamiento de datos de categoría especial sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial y, por descontado, cuando sea necesario por razones de un interés público esencial.

No estará prohibido el tratamiento de datos cuando este tratamiento sea necesario para fines relacionados con la salud de las personas, pero sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario cuando la actividad principal sea la medicina preventiva o laboral, la evaluación de la capacidad laboral del trabajador, el diagnóstico médico o la prestación de asistencia o tratamiento de tipo sanitario o social. Tampoco habrá prohibición cuando el tratamiento de los datos sea necesario para la gestión de los sistemas y servicios de asistencia sanitaria y social.

No regirá la obligación de no tratamiento de datos cuando este tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, así pues, también se incluye como la protección frente a amenazas transfronterizas graves para la salud. También cuando sea preciso actuar sobre las condiciones de los niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios. En todo caso será exigible el secreto profesional y el Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado.

También estarán exentas de la prohibición de tratamiento de datos cuando las actividades principales sean fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. En este orden de cosas, hay que acudir al artículo 89.1 del Reglamento (UE) 2016/679 sobre garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

El "interés público" como base jurídica prevista en el art. 6.1.e) RGPD legitima el tratamiento de datos en determinados casos. Pero tratándose de categorías especiales de datos, el supuesto en el art. 9.2.g) RGPD requiere la concurrencia de un interés público cualificado y, en concreto, un "interés público esencial" habida cuenta de la importancia y necesidad de mayor protección de los datos tratados.

Esta exigencia de un interés público cualificado tiene dos consecuencias. En primer lugar, la excepción a la prohibición general del tratamiento de datos sensibles no puede ser habilitada o regulada por las Autoridades de protección de datos, sino por el legislador (STC 76/2019)[209]. En segundo lugar, el "interés público esencial" implica que

[209] STC 76/2019 de 22 de mayo de 2019 (El Pleno). FJ 2º.

cualquier injerencia en el derecho a la protección de datos debe estar prevista en la ley, responder a una "necesidad social acuciante" en una sociedad democrática y ser proporcional con el fin legítimo perseguido. El TJUE entiende que el criterio de interés general por sí solo no es suficiente para la limitación de un derecho fundamental[210].

En todo caso, cualquier medida que excepcione la prohibición del tratamiento de datos de características especiales deberá ser proporcional al fin perseguido[211], respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Finalmente, en cuanto al acto de consentimiento, no vale cualquier acto sino aquel que reúne las condiciones del artículo 7 del Reglamento (EU) y en especial las del artículo 8 que hace referencia al caso de los menores de edad. Así mismo, el consentimiento no tiene un valor absoluto para el artículo 9 del Reglamento (EU).

5.2. El tratamiento de datos en el contexto de la legislación de protección de datos vigente en la UE

Tal como ya hemos señalado, el dato en sí mismo no tiene valor intrínseco sino cuando este agrupado con otros o cuando en un contexto determinado es capaz de aportar información sobre algo o alguien, es decir, cuando se comporta como un identificador, artículo 4.1 Reglamento (E) 2016/679. A su vez, el dato obtiene relevancia jurídica cuando este tiene el calificativo de dato personal, pero esta relevancia jurídica no viene de la simple existencia del dato personal sino de su tratamiento, es decir, el tratamiento de los datos de las personas, de tal forma que, los datos que no sufren tratamiento están fuera del ámbito de las leyes de protección de datos.

En líneas generales podemos afirmar que cuando la literatura o los textos legales se refieren a gestión de los datos, es sinónimo a utilizar la expresión tratamiento de los datos. Los datos desde que se recogen o reclutan hasta que se eliminan o estacionan pueden sufrir o sufren innumerables operaciones, incluyendo operaciones de trámite y operaciones de uso. Cada uno de las operaciones o procesos de datos tiene sus peculiaridades y sus exigencias. La normativa que protege los datos de las personas denomina a todos estos procesos y operaciones en cualquier tipo de dato, tratamiento de datos.

En los inicios de los años 80 del siglo XX las organizaciones dedicadas a la promoción del bienestar dentro de los parámetros del Estado de Derecho entendían como tratamiento

[210] "En cuanto al carácter necesario de la conservación de datos que impone la Directiva 2006/24, ha de señalarse que es cierto que la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación. Sin embargo, este objetivo de interés general, por fundamental que sea, no puede por sí solo justificar que una medida de conservación como la establecida por la Directiva 2006/24 se considere necesaria a los efectos de dicha lucha." STJUE de 8 de abril de 2014 (Gran Sala) (asuntos C-293/12 y C-594/12), apartado 51, p 19.

[211] ORTEGA KLEIN, A. (12 mayo 2020) "La búsqueda de inmunidad digital frente a la pandemia: eficacia, privacidad y vigilancia". Documento de trabajo 9/2020, 12 de mayo de 2020, Real Instituto Elcano. p 20.

de datos a las operaciones que se realizaban con los datos parcial o totalmente automatizadas, incluyendo desde el registro del dato e inclusión en operaciones matemáticas hasta su borrado o eliminación. El Convenio 108 del Consejo de Europa, de 28 enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, se aprobó en Estrasburgo el 28 de enero de 1981 y fue ratificado por España el 27 de enero de 1984, entrando en vigor de forma general el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo (BOE núm. 274 de 15 noviembre de 1985).

En el año 1999 la LOPD reflejó un cambio de paradigma que había imprimido la propia sociedad, reflejando en su artículo 3 la abismal ampliación del ámbito del concepto de tratamiento de datos, en este orden de cosas dice que: "tratamiento de datos son operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

Aunque, en el año 1995 la Directiva 95/46/CE ya había iniciado el proceso de cambio del concepto de tratamiento de datos personales diciendo que:

> "es cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción."

Lo que empozó tratándose de un interés por el dato automatizado, informático, paso a ser una preocupación por cualquier tipo de dato y en cualquier soporte.

De esta forma el propio Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 define en su artículo 4.2 que tratamiento a efectos del texto jurídico es:

> "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales. Extendiendo esta actividad a procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."

La definición de tratamiento de datos que realiza el Reglamento (UE) 2016/679 no crea ningún tipo de problema ni confusión, pero distinto ocurre con el uso que hace de él tanto el propio Reglamento como la Ley Orgánica 3/2018. No es infrecuente ver que el uso amplio del concepto sufre restricciones en algunos momentos del texto vinculado al uso restrictivo del concepto de dato, pareciendo que en algunos casos se refieren más al ámbito del dato informático que a cualquier otro.

A todo ello, el binomio Reglamento 2016/679 y Ley Orgánica 3/2018 relativo a la protección del dato lo que realmente hacen es regular el tratamiento de los datos limitando de forma importante todo lo relacionado con el mismo, así pues, no es pérdida de tiempo, sino todo lo contario, acudir a la norma para concretar lo que la legislación entiende por tratamiento de datos. De esta forma es el artículo 4, Reglamento 2016/679, el que define ""tratamiento de datos" a efecto del ordenamiento jurídico y a los efectos de la Ley Orgánica 3/2018, pues esta Ley Orgánica no alberga definición alguna.

Una lectura exhaustiva del Reglamento (UE) y la observación del procedimiento de utilización de los datos en cualquier organización nos develan la insuficiencia de esta definición. Además de las operaciones y acciones nombradas por el artículo 4, que en esta Tesis se les dará el apelativo de "Elementos básicos del tratamiento", existen otro tipo de operaciones sobre los datos que no constan en la definición del artículo 4.

Estas operaciones y acciones sobre los datos que no constan en el artículo 4 pero que no por este motivo dejan de afectar, actuar o utilizar al dato son las siguientes: anonimización, seudonimización, bloqueo, circulación, portabilidad, mantenimiento, minimización, exactitud de datos; rectificación, reidentificación, reutilización, tráfico, y transferencia y transmisión internacional. Estas 14 operaciones o acciones no están catalogadas como parte del tratamiento, pero sin duda son parte del tratamiento y en algunos casos aparecen además en el RGPD como derechos o incluso principios. En esta Tesis a este tipo de operaciones o acciones se le denomina "elementos complementarios del tratamiento". En este orden de cosas, como elementos complementarios del tratamiento se entiende: todas las operaciones previas al tratamiento de datos o las operaciones colaterales al tratamiento de datos necesarias para que este sea lícito.

Sin embargo, los elementos básicos y los elementos complementarios del tratamiento no recogen todas las acciones u operaciones adicionales que se pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley Orgánica 3/2018. Este grupo de operaciones o acciones reflejadas en el texto de la norma pero que no se incluyen como elementos básicos o elementos complementarios, en esta Tesis reciben la denominación de "elementos adicionales en el tratamiento de datos".

Por último, y no por ello menos importante, no hay que caer en el error de entender que el Reglamento (UE) y la Ley Orgánica regula solo el tratamiento de dato informático o del de las redes, sino que se refiere a cualquier tipo de dato sea cual sea el soporte que tenga (papel, visual, gráfico, etc.) que sea susceptible de poder llegar a ser incluidos en un fichero o identificar a una persona.

5.3. Tipos de Tratamiento de datos en el Reglamento 2016/679 y Ley Orgánica 3/2018

La mera existencia del RGPD determina a dos grandes grupos de datos, los datos afectados el RGPD y los datos no afectados por dicho reglamento. Dentro del grupo de datos sometidos al régimen del RGPD se debe acudir al artículo 2, sobre el ámbito de aplicación material del Reglamento (UE) 2016/679, que en primer lugar habla de varios tipos de

tratamiento. Por un parte, el tratamiento totalmente automatizado, por otra parte, el tratamiento parcialmente automatizado, y, por último, el tratamiento no automatizado de datos. El Considerando 15 del Reglamento (UE) 2016/679, también nombra el tratamiento manual contraponiéndolo al tratamiento automatizado.

Por otra parte, el artículo 4.2 del Reglamento (UE) 2016/679 entiende que puede haber dos tipos de tratamiento a efectos del Reglamento (UE) 2016/769, el tratamiento automatizado y el tratamiento no automatizado.

En Considerando 15 del Reglamento (UE) 2016/679 determina que la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas.

Resumiendo, se debe entender que se incluyen todos los tratamientos de datos contenidos en ficheros o susceptibles de ser incluidos en ficheros.

Además de las categorías nombradas, tratamiento automatizado y tratamiento manual con sus variantes, como tipos de tratamiento entendemos todas aquellas acciones sobre los datos personales que tanto el Reglamento (UE) 2016/679 como la Ley Orgánica 3/2018 los incluyen en su articulado. También entendemos como tratamiento de datos aquellos requisitos o acciones necesarias para que el tratamiento sea licito y/o exclusivos para dicho fin.

Como elementos básicos del tratamiento consideramos todas las categorías que incluye el artículo 4, definiciones, del Reglamento (UE) 2016/679. Así pues, nos referimos a cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como: "recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."

Como elementos complementarios del tratamiento se entienden todas las operaciones previas al tratamiento de datos o a operaciones colaterales al tratamiento de datos necesarias para que este sea lícito y como elementos adicionales en el tratamiento de datos definimos a las operaciones adicionales que se pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley Orgánica 3/2018.

5.3.1. Elementos básicos del tratamiento de datos

Los elementos básicos del tratamiento de datos son todas las operaciones directas sobre datos que se pueden producir sobre los datos personales y que requieren de protección por parte del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 y que aparecen en el punto 2) del artículo 4, sobre definiciones, del Reglamento (UE) 2016/679. Estas operaciones o acciones que venimos a llamar elementos básicos del tratamiento son: "recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción." A continuación, se detallan de una en una:

5.3.1.1. Acceso

El acceso, entendido por la RAE como acción de entrada o paso, es la primera expresión que manifiesta la definición de tratamiento de datos. Es más que evidente que para tratar un dato se debe primero acceder a él. El Reglamento (UE) 2016/679 y La Ley Orgánica 3/2018 hace referencia al acceso tanto como un derecho como paso o proceso inicial de entrada.

El Reglamento (UE) 2016/679, en su artículo 4, define el acceso como una parte del tratamiento al decir que el tratamiento es:

> "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."

Este texto legislativo en su artículo 32, sobre seguridad del tratamiento, trata el acceso como la acción necesaria para llegar a los datos.

La Ley Orgánica 3/2018 hace la primera referencia al acceso como una acción o tratamiento, se expresa en artículo 24, sobre sistemas de información de denuncias internas, limitando y regulando las personas que pueden entrar en dichos sistemas de información.

El legislador da un paso más al hablar incluso de "régimen de acceso", es decir, el conjunto de normas o reglas que rigen, cuando se refiere a la entrada de la Administración pública en los archivos de interés público en relación a las condiciones que considera lícitas para el tratamiento de archivos. Concretamente es el artículo 26 de la Ley Orgánica 3/2018, sobre tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas, el que dice "será lícito el tratamiento" para luego añadir el régimen de acceso que regula el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso.

El artículo 33, del encargado del tratamiento, de la Ley Orgánica 3/2018, también utiliza el término "acceso" como una acción que puede llevar a cabo el encargado del tratamiento de datos personales.

También es cierto que el artículo 36, sobre posición del delegado de protección de datos, de la Ley Orgánica 3/2018 en su punto 3 distingue entre acceso a los datos personales y los procesos de tratamiento al decir:

> "En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica".

Esta diferenciación se puede deber a un simple recurso semántico para reforzar el "acceso" dentro de las múltiples operaciones que se pueden dar dentro del tratamiento de datos.

El artículo 49, sobre el Consejo Consultivo de la Agencia Española de Protección de Datos, de la Ley Orgánica 3/2018 hace mención al acceso como una acción de entrada o llegada, al hablar en su punto n) de "expertos en transparencia y acceso a la información pública".

El artículo 53, sobre alcance de la actividad de investigación, dentro de la Sección 2.ª Potestades de investigación y planes de auditoría preventiva del Capítulo I, de La Agencia Española de Protección de Datos, de Título VII, sobre Autoridades de protección de datos, de la Ley Orgánica 3/2018, en su punto 2, se refiere al acceso como a una acción, concretamente dice: "Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio constitucionalmente protegido del inspeccionado, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial."

A todo ello hay que añadir que el derecho de acceso deberá entenderse como un acceso razonable[212], expresión utilizada por el artículo 6 de la Directiva 95/46/CE[213].

5.3.1.2. Adaptación y modificación

Adaptación, según la RAE, es la acción o efecto de adaptar. Adaptar, para la RAE, es la acción o el efecto de acomodar o ajustar algo. Al referirnos a los datos, se entiende como un cambio en el registro por motivos de que ha cambiado la realidad que los soporta, es decir, sería motivo de adaptación el dato sobre la estatura de una persona o su edad. Es decir, presupone que el dato que es preciso cambiar estaba correcto previamente, tan solo que ya no corresponde a la realidad de la persona física pues esta ha cambiado. Otras palabras sinónimas serían ajuste o acomodación.

Modificación, según la RAE, es la acción o efecto de modificar. Siendo modificar, según la RAE, transformar o cambiar algo mudando alguna de sus características. Cuando hace referencia a datos simplemente significa cambiar un dato por otro, sin más. Otras palabras sinónimas serían cambiar, variar, reformar o enmendar.

El Reglamento (UE) 2016/679, define como tratamiento de datos personales, entre otras cosas, a la adaptación o modificación de datos personales. Es concretamente en el punto 2 del artículo 4, sobre definiciones, en donde incluye a estos procesos dentro de la definición de tratamiento de datos personales.

La Ley Orgánica 3/2018, también manifiesta en uno de sus preceptos que una de las actividades del tratamiento es la modificación del contenido de un registro. Concretamente la Ley Orgánica 3/2028 en su artículo 37, del registro de las actividades de tratamiento, en el párrafo tercero del punto uno dice: "Cuando el responsable o el encargado del

[212] STS 2484/2019 de 12 de julio de 2019 (Sala de los Contencioso). FD 3º.

[213] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro."

5.3.1.3. Conservación

La RAE define conservación como la preservación de algo o el mantenimiento de efectos. A su vez podemos entender por conservación la acción de conservar, en cuyo caso cabe decir que para la RAE conservar es mantener o cuidar de la permanencia o integridad de algo o de alguien o guardar con cuidado algo.

El Reglamento (UE) entiende la conservación como uno de los elementos del tratamiento, cuando en su artículo 4 dice que se entiende por tratamiento a: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como ……, conservación, …….. "

Además, hace referencia al acto de conservar datos como al acto de mantenerlos y lo vincula al tiempo de conservación y con la responsabilidad del responsable del tratamiento[214]. En el artículo 6, sobre licitud del Tratamiento, hace referencia a la limitación del plazo de conservación, de los datos.

El artículo 15, del derecho de acceso del interesado, estipula que este derecho de acceso lo es también de que el interesado conozca "el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo".

La Ley Orgánica 3/2018 se refiere al acto de conservar datos (o registros) como una de las funciones del encargado del tratamiento de los datos. El texto legal también hace mención a la conservación vinculándolo al tiempo y en especial cuando este tiempo está vinculado a la existencia de los datos de una persona física en una base de datos y más todavía si esta se incluye en el artículo 24, sobre sistemas de información de denuncias internas.

La conservación de los datos fue regulada por Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Esta Directiva fue anulada por el Tribunal de Justicia de la Unión Europa por contravenir dos derechos fundamentales de la Carta de Derechos Fundamentales de la unión europea por entender que era una injerencia adicional en

[214] "Del mismo modo, resulta relevante mencionar el caso Schwartz, en el cual el TJUE consideró que la toma de impresiones dactilares por parte de las autoridades nacionales correspondientes, para su conservación en el dispositivo de almacenamiento integrado en el pasaporte, cabe dentro del concepto de tratamiento de datos de carácter personal" QUESADA MONGE, DF. (2017) "Transparencia administrativa, acceso a la información y protección de datos personales: criterios para una conciliación de derechos desde la jurisprudencia del TJUE y la Ley 19/2013, de 9 de noviembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno". Tesis Doctoral. Faculta de Derecho. Universidad Autónoma de Madrid. Madrid. España.

los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal[215].

5.3.1.4. Comunicación y difusión

Por comunicación la RAE define la acción y efecto de comunicar o comunicarse; transmisión de señales mediante un código común al emisor y al receptor.

Por difusión la RAE define la acción o efecto de difundir. A su vez definimos como difundir propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc.

En este punto sobre comunicación y difusión es preciso referirse al principal medio de difusión en la actualidad, es decir, a internet. En este sentido, se deberán tener en cuenta cuales son fuentes de acceso público y cuales no lo son, en cada caso y en cada momento. La AEPD ha dejado muy claro que las sentencias judiciales no son fuente de datos accesibles al público[216].

El Reglamento (UE) incluye los conceptos de comunicación y difusión en la propia definición de tratamiento cuando expone en su artículo 4 que tratamiento es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, (…) comunicación por transmisión, difusión o cualquier otra forma de habilitación (…)".

El Reglamento (UE) vincula la comunicación como uno de los posibles tratamientos de los datos personales a la licitud del tratamiento a través de su limitación, tal se desprende del artículo 6, sobre licitud del tratamiento.

En cuanto al término comunicación, la Ley Orgánica 3/2018 lo define como parte del tratamiento de datos y en consecuencia una operación que debe ser regulada bajo el paraguas del Reglamento (UE) en varios de sus artículos.

La Ley Orgánica 3/2018 utiliza el término comunicación dentro del contexto general de la expresión. El artículo 21.1, sobre tratamientos relacionados con la realización de determinadas operaciones mercantiles, utiliza el término comunicación haciendo referencia al tratamiento de los datos, así pues, dice: "Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del (…)".

Por otra parte, el artículo 24.2, de sistemas de información de denuncias internas, también utiliza el vocablo comunicación dentro del contexto del tratamiento de datos. Concretamente dice: "(…) No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan."

[215] STJUE de 8 de abril de 2014 (Gran Sala) (asuntos C-293/12 y C-594/12), apartados 34 a 37, 39, 47 a 48, 56, 60, 65.
[216] AEPD (2000) "Memoria de la Agencia Española de Protección de Datos". p 115.

El artículo 25.2, sobre tratamiento de datos en el ámbito de la función estadística pública, utiliza de nuevo el término comunicación como una acción propia del tratamiento de datos al referirse a: "La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos (…)".

El artículo 33.1, sobre el encargado del tratamiento, utiliza el término comunicación para hacer mención a una situación en la que la comunicación de datos no se considerará tratamiento de datos aplicable al Reglamento (UE) 2016/679, manifestándolo de la siguiente manera:

> "El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente Ley Orgánica y en sus normas de desarrollo."

El artículo 52.1., sobre el deber de colaboración, indica cuando la comunicación de datos estará bajo la aplicación del Reglamento (UE) 2016/679, expresando: "Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación."

Cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

En cuanto al término difusión, la Ley Orgánica 3/2018 no lo define como parte del tratamiento de datos.

5.3.1.5. Cotejo

Por cotejo la RAE entiende la prueba consistente en la acreditación de la autenticidad de un documento, ya sea mediante la confrontación del documento con su original, ya sea mediante el contraste de letras, operación que se lleva a cabo por un perito designado por el juez. En términos generales, se pude entender como cotejo aquel procedimiento que permite acreditar la autenticidad de algo mediante un acto de comparación.

El Reglamento (UE) incluye el término de cotejo en la propia definición de tratamiento cuando expone en su artículo 4 que tratamiento es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, ….. o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."

La Ley Orgánica 3/2018, no utiliza este término.

5.3.1.6. Destrucción

La RAE entiende por *destrucción* la acción o efecto de destruir. A su vez destruir, según la RAE, se define como reducir a pedazos o a cenizas algo material, u ocasionarle un grave daño; deshacer o inutilizar algo no material.

El Reglamento (UE) incluye el término de destrucción en la propia definición de tratamiento cuando expone en su artículo 4 que tratamiento es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, (…), limitación, supresión o destrucción."

El sentido en el que trata el Reglamento (UE) el término destrucción en el contexto de la protección de datos personales, es precisamente la seguridad de los mismos en cuanto su seguridad, artículo 4, sobre definiciones, en este orden, para el Reglamento (UE) violación de la seguridad de los datos personales es toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

El artículo 5, de principios relativos al tratamiento, del Reglamento (UE) 2016/679 entiende que la seguridad es uno de los principios del tratamiento. En cuando a los datos personales, el artículo 5 indica en su letra f) de su punto 1, que

> "los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)"

El artículo 32, sobre seguridad del tratamiento, del Reglamento (UE) 2016/679 en su punto dos, dice:

> "Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

De tal forma el Reglamento (UE) no fija la destrucción como paso u operación del tratamiento de datos, sino que lo utiliza para indicar los niveles de seguridad que se deben tomar para evitar la destrucción como consecuencia.

La Ley Orgánica 3/2018, a diferencia del Reglamento (UE) trata el término destrucción como una operación más, la última, que se puede o debe realizar sobre los datos de personas en el procedimiento de su tratamiento. Es decir, la destrucción la entiende como parte autónoma del tratamiento.

El artículo 32, sobre bloqueo de los datos, de la Ley Orgánica 3/2018 determina que, tras el bloqueo de datos personales, transcurrido el plazo de prescripción exigido por la norma correspondiente para algunos documentos utilizados por los jueces,

magistrados, Ministerio Fiscal o Administración pública deberá procederse a la destrucción de estos. A lo que el artículo 33, sobre el encargado del tratamiento, en su punto 3 añade:

> "el responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.
>
> No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista."

5.3.1.7. Extracción, consulta y utilización

La RAE entiende por *extracción* la acción o efecto de extraer. A su vez, la RAE define como extraer, sacar o poner algo fuera de donde estaba.

La RAE entiende por *consulta* la acción o efecto de consultar. A su vez consultar, según la RAE, es buscar documentación o datos sobre algún asunto o materia.

La RAE entiende por *utilización* la acción o efecto de utilizar. A su vez utilizar, para la RAE es hacer que algo sirva para un fin.

El Reglamento (UE) incluye el término de extracción, de consulta y de utilización en la propia definición de tratamiento cuando expone en su artículo 4 que tratamiento es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como (…), extracción, consulta, utilización, (…)".

El Reglamento (UE) utiliza el término consulta para dos significados distintos. Por una parte, utiliza el término consulta previa en el artículo 36 como un trámite administrativo que podrá realizar el responsable del tratamiento frente a la Autoridad de control cuando una evaluación de impacto relativa a la protección de los datos, en virtud del artículo 35, muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo. Por otra parte, utiliza el término consulta como una operación del tratamiento datos personales como aquella acción que lleva a conocer un dato personal, así pues el Considerando 111 dice: "(…) cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas (…)".

El artículo 49, de excepciones para situaciones específicas, hace referencia a la utilización de consulta como la acción de consultar para conocer, al decir: "g) (…), tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, (…)".

Tan solo algún Considerando utiliza el término "utilización" como una acción dentro del tratamiento de datos personales. Concretamente el Considerando 38 dice: "a la utilización de datos personales (…)" Otro Considerando que hace lo mismo es el 116, dice: (…) protegerse contra la utilización o comunicación ilícitas de dicha información".

La Ley 3/2018 no utiliza el término extracción.

La Ley 3/2018 utiliza el término consulta en el sentido de buscar para conocer o contrastar en el artículo 20, sobre sistemas de información crediticia.

La Ley 3/2018 usa el término "utilizar" en el sentido de usar un dato en la Disposición final tercera, sobre modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, al mencionar "se podrán utilizar datos personales".

5.3.1.8. Interconexión

La RAE entiende por *interconexión* la acción o efecto de interconectar. A su vez interconectar se define como la acción u operación de conectar dos o más elementos entre sí.

El Reglamento (UE) incluye el término de *interconexión* en la propia definición de tratamiento cuando expone en su artículo 4 que tratamiento es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como (…), cotejo o interconexión, (…)".

El Reglamento (UE) en su Considerando 33, hace una referencia a interconexión cuando entiende que las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros.

La Ley Orgánica 3/2018 no hace referencia a la interconexión como operación posible con los datos personales.

5.3.1.9. Limitación

Por limitación la RAE define la acción o efecto de limitar o limitarse. En este orden de cosas la RAE entiende por limitar como poner límites a algo; acortar o ceñir.

El Reglamento (UE) 2016/679 en su artículo 4, definiciones, presenta una definición sobre la limitación en el tratamiento, dice: "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro."

El Reglamento (UE) utiliza el término limitación en varios sentidos. Por una parte, en cuanto a operaciones o acciones en su tratamiento; por otra parte, en cuanto a limitación de la finalidad, artículo 5.1.b) y artículo 6.3.b); por otra parte, en cuanto a limitación del plazo de conservación, artículo 5.1.e); por otra parte, la limitación de su tratamiento, artículo 13.2.b) y artículo 15.1.e); por otra parte, en el llamado derecho a la limitación del tratamiento, artículo 18 y artículo 19.

El Reglamento (UE) en su artículo 23, sobre limitaciones, estipula que el Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y

obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar las materias y circunstancias que refleja el propio artículo 23.

La Ley Orgánica 3/2018, en su artículo utiliza el término limitación para expresar el derecho a la limitación del tratamiento, al cual hace referencia también el artículo 20, sobre sistemas de información crediticia, el artículo 73, de infracciones consideradas graves, y el artículo 74, sobre infracciones consideradas leves.

Concluyendo, la acción u operación que hace efectiva la voluntad de oponerse conlleva un tratamiento del dato encaminado a cumplir tal efecto, es decir, la limitación al acceso o al tratamiento general de un dato o la oposición a cualquier tratamiento de un dato conlleva en sí mismo un tratamiento específico encaminado a tal objetivo.

5.3.1.10. Organización y estructuración

La RAE entiende por organización, la acción o efecto de organizar. A su vez organizar, se define como la acción u operación de poner algo en orden; hacer, producir algo; establecer o reformar algo para lograr un fin, coordinando las personas y los medios adecuados.

La RAE entiende por estructuración la acción o efecto de estructurar. A su vez estructurar, se define como la acción u operación de articular, distribuir, ordenar las partes de un conjunto.

El Reglamento (UE) 2016/679 define en su artículo 4, definiciones, lo que entiende en el ámbito de este el concepto de tratamiento. En este orden de cosas, incluye en la definición las acciones u operaciones de organizar y de estructurar, diciendo que es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, (…)".

El Reglamento (UE) utiliza el término organizar en muchas ocasiones al referirse a organización internacional o a organización como sustantivo y no como verbo indicativo de acción u operación. Tan solo en una ocasión hace referencia a organización como indicativo de acción u operación, en el Considerando 158.

El Reglamento (UE) no utiliza el término estructuración como acción de estructurar en ninguna ocasión.

La Ley Orgánica 3/2018, no utiliza los términos organización y estructuración en el sentido de acción de organizar o estructurar en ninguna ocasión.

5.3.1.11. Recogida y registro (de datos)

La RAE entiende por *recogida* la acción o efecto de recoger. A su vez recoger, se define como la acción u operación de hacer la recolección de los frutos, coger la cosecha; guardar, alzar o poner en lugar seguro algo. También por recogida se entiende anotación, captura o acción de coger.

La RAE entiende por *registro de datos* la acción o efecto de registrar datos. A su vez registrar datos, se define como la acción u operación de anotar datos.

El Reglamento (UE) 2016/679 define en su artículo 4, definiciones, lo que entiende en el ámbito de este el concepto de tratamiento. En este orden de cosas, incluye en la definición las acciones u operaciones de recogida y registro de datos, diciendo que es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, ……"

El Reglamento (UE) en su artículo 40, de Códigos de conducta, hace referencia a que el objeto de los códigos de conducta será el de especificar la aplicación del presente Reglamento, de distintos conceptos, extremos o categorías, entre las cuales se incluye la recogida de datos personales.

El Reglamento (UE) hace referencia a la recogida de datos como a la acción de anotar o coger datos de personas en los Considerandos 6, 33, 35, 39, 47, 50 y 162.

El Reglamento (UE) utiliza el término *registro,* en su acepción de archivo, en su articulado. Es en el Considerando 62 en el que utiliza el este término como la acción de registrar o anotar.

La Ley Orgánica 3/2018 en el artículo 28.2 (Obligaciones generales del responsable y encargado del tratamiento) utiliza el término recogida en el sentido de una acción u operación de captura de datos, en este sentido dice:

> "Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos …… f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales."

La Ley Orgánica 3/2018, utiliza el término registro en el sentido de acción u operación del tratamiento de datos en el artículo 3 (Datos de las personas fallecidas) al referirse en su punto 2:

> "Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello (…) Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos."

La Ley Orgánica 3/2018, utiliza mayormente en su articulado el término registro en la acepción de lugar y no de acción.

5.3.1.12. Supresión

La RAE entiende por *supresión* la acción o efecto de suprimir. A su vez suprimir, se define como la acción u operación de hacer cesar, hacer desaparecer.

El Reglamento (UE) 2016/679 define en su artículo 4, definiciones, lo que entiende en el ámbito del mismo el concepto de tratamiento. En este orden de cosas, incluye en la

definición las acciones u operaciones de recogida y registro de datos, diciendo que es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como ……., supresión o destrucción"

El Reglamento (UE) 2016/679 utiliza en muchas ocasiones el término supresión como derecho y en algunas ocasiones lo hace directamente como acepción de suprimir y en varias de ellas con alusión directa al tratamiento. Así el artículo 17.1 (Derecho de supresión («el derecho al olvido»)), dice que el responsable del tratamiento tendrá la obligación de suprimir los datos de una persona cuando esta se lo pida, diciendo:

> "El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:"

El Reglamento (UE) en su artículo 30.1 (Registro de las actividades de tratamiento) hace mención directa al concepto de supresión como acción u operación del tratamiento, cuando dice:

> "Cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación: f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;"

La Ley Orgánica 3/2018, hace mención directa y explícita a la supresión como parte del tratamiento de datos en el artículo 21 (Tratamientos relacionados con la realización de determinadas operaciones mercantiles) al mencionar en su punto 2: "En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica."

5.3.2. Elementos complementarios del tratamiento de datos

En el epígrafe anterior se describen los elementos básicos del tratamiento de datos en el Reglamento (UE) 2016/679 y se definen como todas las operaciones y acciones incluidas en su artículo 4.2), definiciones. En este epígrafe se describen y definen los elementos complementarios del tratamiento, que son todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4.2), definiciones, del Reglamento (UE) 2016/679, pero que son: acciones u operaciones previas al tratamiento de los datos personales; o acciones u operaciones colaterales al tratamiento de datos; o que son acciones u operaciones necesarias para que este tratamiento sea lícito.

Los elementos complementarios del tratamiento de datos son las siguientes acciones: anonimización y seudonimización; bloqueo; circulación y portabilidad; mantenimiento; minimización; exactitud de datos; rectificación; reidentificación; reutilización; tráfico; y transferencia y transmisión internacional.

5.3.2.1. Anonimización y seudonimización

Anonimización, según la RAE, es la acción de expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad. Mientras que la seudonimización es un procedimiento de gestión de datos donde se reemplazan campos de información personal dentro de un registro de datos por uno o más identificadores artificiales o pseudónimos (AEPD, 2019)[217]. La seudonimización es otra alternativa a la anonimización de datos.

La Ley 14/2007, de 3 de julio, de investigación biomédica define por anonimización como "proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere", Artículo 3 c) de la Ley 14/2007, de 3 de julio, de investigación biomédica. La misma Ley define como dato anonimizado:

> "dato que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados", Artículo 3 i) de la Ley 14/2007, de 3 de julio, de investigación biomédica.

El Reglamento (UE) 2016/679 no utiliza el término anonimizar. El concepto anónimo tan solo lo utiliza en su Considerando 26, al hacer referencia a que el Reglamento no se debe aplicar a los datos anónimos ni a los datos personales convertidos en anónimos.

Para el Reglamento (UE) 2016/679 la seudonimización (artículo 4) es:

> "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable."

Tanto la anonimización como la seudonimización no tan solo es parte del tratamiento que se deben dar a los datos personales, sino que, en determinados supuestos, es condición previa para su licitud cuando no ha mediado consentimiento, Artículo 6.4 del Reglamento (UE) 2016/679. Sin embargo, tal como expresa el Considerando 28, su introducción explícita en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

El artículo 6, sobre licitud del tratamiento, del Reglamento (UE) 2016/679, entiende que la seudonimización es una condición que hace lícito el tratamiento de datos personales y el artículo 32, seguridad del tratamiento, entiende que la seudonimización es junto con el cifrado, la primera técnica de seguridad que hay que aplicar a los datos personales para su tratamiento.

[217] AEPD (2019) "Análisis de riesgos y adopción de medidas de seguridad". Octubre 2019. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/analisis-de-riesgos (31/01/2021).

El Reglamento (UE) 2016/679 utiliza el concepto de seudonimización y explica el alcance del mismo. En su Considerando 26, dentro de la protección de los datos personales, dice que aquella seudonimización que mediante información adicional permite conocer a la persona física no exime de la aplicación de todas las normas de protección de datos personales aplicables a persona identificable.

El Reglamento (UE) 2016/679 determina que los Códigos de Conducta, del artículo 40, pueden estipular sobre la seudonimización de los datos personales.

El Reglamento (UE) 2016/679 entiende por la seudonimización de los datos personales como una medida técnica y organizativa de garantía, la cual es mencionada en el punto 1 del artículo 89 cuando el Reglamento trata las "Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos", dentro del Capítulo IX, sobre disposiciones relativas a situaciones específicas de tratamiento.

La Ley Orgánica 3/2018, hace una breve mención al concepto de anonimización en el artículo 72 y hace mención a los dos conceptos en la Disposición adicional decimoséptima, sobre el tratamiento de datos de salud. Concretamente, habla de anonimización y seudonimización en cuando en la letra f) del punto 2 se refiere a que deben evaluarse los riesgos de la reidentificación de los datos anonimizados o seudonimizados. Así pues, en su punto f) al referirse al tratamiento con fines de investigación en salud pública y, en particular, biomédica, dice que se procederá a realizar una evaluación de impacto que incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

La Disposición adicional decimoséptima, tratamientos de datos de salud, hace mención solo al término seudonimización, en la lera d) del punto 2, el tratamiento de datos en la investigación en salud se regirá por los siguientes criterios, cuando dice que la seudonimización da licitud al uso de datos personales con fines de investigación en salud y, en particular, biomédica.

A su vez, la letra d) del punto 2, no significa barra libre cuando se han seudonimizado los datos personales en procesos de investigación biomédica, sino que deben darse los siguientes requisitos:

> "i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
>
> ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados."

Los condiciones o posibilidades para la reidentificación en el contexto de la Disposición adicional decimoséptima se determinan por lo dispuesto en la letra d) del punto 2, al decir:

> "podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una

> amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria."

Por último, el artículo 72, sobre infracciones consideradas muy graves, habla de la reversión deliberada de la anonimización cuando se persigue la reidentificación de las personas físicas, como una infracción muy grave.

La anonimización de los datos personales, siendo un elemento complementario del tratamiento de los datos también puede aparecer como un derecho vinculado al derecho de supresión de datos personales. Esta connotación de derecho a la supresión de un dato personal anonimizando el mismo puede entrar en colisión con otro derecho fundamental como es el de libertad de prensa del artículo 20 de la Constitución. La Sala primera del Tribunal Constitucional el 4 de junio de 2018 dijo al respecto en el caso concreto de ese recuro de amparo que "Esta opción, que supondría una injerencia más intensa en la libertad de prensa que la simple limitación en la difusión, resulta por tanto innecesaria. Y, descartada la necesidad de la medida, huelga toda consideración en torno a la proporcionalidad en sentido estricto de la misma"[218].

5.3.2.2. Bloqueo

Se entiende por bloqueo, según la RAE, la acción o efecto de bloquear. Por otra parte, la RAE define el término bloquear como la acción de interceptar, obstruir o cerrar el paso; impedir el funcionamiento normal de algo; dificultar, entorpecer la realización de un proceso.

El Reglamento (UE) 2016/679 no utiliza este término. Sin embargo, la Ley Orgánica 3/2018, si utiliza el término bloqueo y concretamente se atribuye no tan solo a un tratamiento convencional sino a un tratamiento especial. La doctrina del Tribunal de Justicia de la Unión Europea también entiende al bloqueo como una técnica en el tratamiento de los datos[219].

La Ley Orgánica 3/2018, en el punto dos del artículo 32 entiende por bloqueo de los datos:

> "la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas".

A esta acción del tratamiento de los datos personales le confiere la naturaleza de obligación, así pues, el punto uno del artículo 32 determina que el responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

La acción de bloquear podrá ser acordada por la Agencia Española de Protección de Datos, artículo 69 de la Ley Orgánica 3/2018, como medidas provisionales necesarias y

[218] STC 58/2018, de 4 de junio de 2018 (Sala Primera). FJ 8º.

[219] STJUE de 24 de septiembre de 2019 (Gran Sala), (asunto C-507/17) apartados 39 y 43.3, p 14.

proporcionadas para salvaguardar el derecho fundamental a la protección de datos, en concordancia con el artículo 66, sobre procedimiento de urgencia, del Reglamento (UE) 2016/679.

5.3.2.3. Circulación y portabilidad

Circulación, según la RAE, es la acción de circular. A su vez, la RAE entiende por circular, ir y venir, pasar algo de unas personas a otras.

Portabilidad, hace referencia a portable como aquella cualidad que tiene un objeto, elemento o casa que es posible, fácil o sencillo de mover de un lugar a otro, es sinónimo de portátil. Portabilidad y circulación, son dos conceptos que van estrechamente unidos y más si cabe en el contexto de la normativa sobre la protección de datos personales y sobre la libre circulación de los mismos.

La circulación de los datos, entendida como un derecho de la persona dentro de la Unión Europea, aparece no tan solo como una acción sobre el dato, como un tratamiento del mismo, sino como un principio en el que se sustenta el Reglamento (UE) 2016/679. Es en el punto uno del artículo 1, sobre el objeto del RGPD, que dice: "El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos". A lo cual se añade en el punto tres: "La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales". No en vano el título del Reglamento (UE) es precisamente: 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).

La Ley Orgánica 3/2018, en la misma línea que el Reglamento (UE), en el artículo 1, objeto de la ley, hace explica mención a la libertad de circulación de datos personales.

El Reglamento (UE) 2016/679, define en su artículo 20, sobre el derecho a la portabilidad de los datos, la portabilidad al hacer referencia al derecho a la portabilidad de los datos. En este orden de cosas, para el Reglamento (UE) portabilidad es:

> "recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado."

La Ley Orgánica 3/2018, al referirse al derecho de portabilidad direcciona el artículo 17 al artículo 20 del Reglamento (UE) 2016/679.

5.3.2.4. Exactitud de los datos

Por exactitud la RAE define como la cualidad de exacto. En este orden de cosas la RAE entiende por exacto como lo dicho de una palabra o de un texto que es literal, igual que el otro.

El Reglamento (UE) en su artículo 5, de principios relativos al tratamiento, hace referencia a que los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan, exactitud. De esta forma, los procedimientos, operaciones o sistemas que busquen la exactitud del dato deberán entenderse como tratamiento de datos, pues si aparece como un principio para la búsqueda del mismo es preciso actuar en este sentido.

El Reglamento (UE) en el artículo 18, del derecho a la limitación del tratamiento, utiliza el término exactitud al referirse a que se deberá verificar la exactitud de los mismos. En este orden de cosas, la exactitud requerirá de operaciones como es su verificación.

La Ley Orgánica 3/2018, también hace referencia a este término en su artículo 4, de exactitud de los datos, dentro del Título II sobre Principios de protección de datos.

5.3.2.5. Mantenimiento

La RAE define mantenimiento como la acción y efecto de mantener o mantenerse. A su vez podemos entender por mantener como la acción de conservar algo en su ser, darle vigor y permanencia, en cuyo caso cabe decir que para la RAE mantener es cuidar de la permanencia o integridad de algo o de alguien o guardar con cuidado algo.

El Reglamento (UE) hace referencia al acto de conservar datos como al acto de mantenerlos y lo vincula al tiempo de conservación y con la responsabilidad del responsable del tratamiento. En el artículo 6, de licitud del tratamiento, hace referencia a la limitación del plazo de conservación, de los datos.

La RAE define mantenimiento como acción de mantenerse o mantener; conjunto de operaciones y cuidados necesarios para que instalaciones, edificios, industrias, etc. … puedan seguir funcionando correctamente. También se entiende mantenimiento como las acciones que permitan restaurar a un estado en el cual pueda llevar a cabo alguna función requerida[220].

El Reglamento (UE) no utiliza este término.

La Ley Orgánica 3/2018 utiliza el término mantenimiento como aquella acción que permite la permanencia de un dato en un sistema. En el artículo 34, sobre designación de un delegado de protección de datos, estipula que el responsable del tratamiento deberá nombrar a un delegado de protección de datos en: “l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes”. De esta forma, la norma entiende el manteniendo de los datos como parte del tratamiento que se debe dará a estos y que a su vez se enmarca dentro de las obligaciones relativas a los responsables del tratamiento.

Este concepto de mantenimiento vuelve a aparecer al definir una de las acciones naturales de los profesionales de la salud y que a su vez definen sus obligaciones, así pues, “estando

[220] AEC. (mayo 2020) “Mantenimiento”. Disponible en https://www.aec.es/web/guest/centro-conocimiento/ mantenimiento (31/01/2021).

legalmente obligados al mantenimiento de las historias clínicas" en orden a determinar que quedan exentos de la obligación de nombrar a un delegado de protección de datos cuanto esta actividad sea a título personal, es decir, en las consultas privadas de los profesionales de la salud que ejerzan esta modalidad de actividad profesional.

5.3.2.6. Minimización

Por minimización la RAE define la acción o efecto de minimizar. En este orden de cosas la RAE entiende por minimizar la acción de reducir lo más posible el tamaño de algo.

El Reglamento (UE) 2016/679 en su artículo 5, sobre principios relativos al tratamiento, al referirse a minimización de datos, expresa que los datos deberán ser adecuados, pertinentes y limitados a lo necesario, es decir, que los datos no se recogerán si no fuera necesario hacerlo. Por otra parte, esta necesidad no se deja a la libre voluntad de quien desee recogerlos sino a aquella necesidad que venga dada por los fines de la actividad que precisa su tratamiento.

El Reglamento (EU) 2016/679 en su artículo 25, protección de datos desde el diseño y por defecto, entiende que el responsable del tratamiento aplicará el criterio de minimización de datos, lo cual tendrá presente en cuando determine los procesos o elementos básicos del tratamiento y en el momento de utilizarlo adoptando las técnicas y organización preceptivas.

El Reglamento (EU) 2016/679 en su artículo 47, sobre normas corporativas vinculantes, incluye a la minimización de datos como uno de los principios generales de la protección de datos a tener en cuenta a la hora de definir las normas corporativas vinculantes.

La Ley Orgánica 3/2018, no utiliza el término minimización ni minimizar.

5.3.2.7. Rectificación

La RAE define rectificación como la acción o el efecto de rectificar. A su vez podemos entender por rectificar es la acción modificar algo dicho o hecho previamente.

La rectificación aparece también como un derecho en el Reglamento (UE) 2016/679, concretamente en el artículo 16, sobre el derecho a rectificación.

La Ley Orgánica 3/2018, también presenta la rectificación como un derecho, así lo expresa el artículo 14, derecho de rectificación.

Sin duda, también debe entenderse como un tipo de tratamiento dado que las operaciones o acciones para rectificar un dato no son sencillas y requieren de acciones u operación para verificar, borrar o eliminar e introducir nuevos datos donde estaban los que se han rectificado.

5.3.2.8. Reidentificación

La RAE define identificación como la comprobación de la identidad de una persona. También la RAE entiende por identificación a la fase de tratamiento archivístico que consiste en la investigación y sistematización de las categorías administrativas y

archivísticas en que se sustenta la estructura de un fondo. Para la RAE el prefijo "re" se utiliza para significar repetición.

Por el contenido de la Ley Orgánica 3/2018, por reidentificación se entiende la acción de identificación de alguien que ya había sido identificado y que por circunstancias diversas su identidad había sido eliminada o imposible de conocer.

El Reglamento (UE) 2016/679 no utiliza el término de reidentificación, sin embargo, la Ley Orgánica 3/2018 si lo hace.

La Ley Orgánica (UE) 2016/679 en su artículo 72 (Infracciones consideradas muy graves) ubicado en el Titulo IX (Régimen sancionador) en relación al término reidentificación dice: "p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados". En este orden de cosas, para la Ley 3/2018 reidentificación consiste en volver a identificar a una persona cuando esta había sido anonimizada.

La Disposición adicional decimoséptima (Tratamientos de datos de salud) de la Ley Orgánica 3/2018 vuelve a utilizar el término reidentificación cuando en aparado 1ª de la letra d) del punto 2 dice: "El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá: 1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación".

El apartado 2º del precepto al que se refiere el párrafo anterior dice:

> "2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:
>
> i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
>
> ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados."

La propia Disposición adicional decimoséptima de la Ley Orgánica 3/2018 utiliza el término reidentificación en más casos, con el mismo sentido.

5.3.2.9. Reutilización

La RAE define utilizar como hacer que algo sirva para un fin. También la RAE entiende por reutilizar volver a utilizar algo, bien con la función que desempeñaba anteriormente o con otros fines. En este orden de cosas reutilización es la acción o resultado de utilizar algo ya utilizado previamente y lo mismo con la palabra reutilización. Para la RAE el prefijo "re" se utiliza para significar repetición.

El Reglamento (UE) usa el término utilización dentro de la definición de tratamiento de datos en su artículo 4, definiciones, ya tratado en páginas anteriores. Es decir, utilizar un dato se entiende como parte o fase posible del tratamiento de los datos personales.

El Reglamento (UE) no usa el término reutilización de datos en su articulado, pero si lo hace en sus Considerandos. Concretamente el Considerando 154 dice: "Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales" y dirige al lector interesado a la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p. 90).

La Ley Orgánica 3/2018 incluye el término reutilización en la Disposición adicional decimoséptima, sobre tratamientos de datos de salud, concretamente en su punto 2 al manifestar que:

> "Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial."

La Disposición transitoria sexta, sobre reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica, de la Ley Orgánica 3/2018 entiende, además, que se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta Ley Orgánica cuando concurra alguna de las circunstancias siguientes:

> "a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento. b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial."

5.3.2.10. Tráfico

Por tráfico la RAE define flujo de datos a través de la red.

El Reglamento (UE) no utiliza el término tráfico.

En cuanto al término tráfico, la Ley Orgánica 3/2018 lo define como parte del tratamiento de datos.

El preámbulo de la Ley Orgánica utiliza el término tráfico para hacer referencia al uso mediante trasiego de los datos, en ese sentido se remite a la Sentencia 94/1998, de 4 de mayo[221] del Tribunal Constitucional en la cual reconoce el derecho de las personas a evitar el tráfico de sus datos, como derecho fundamental que es la protección de los datos personales, con el siguiente tenor literal "para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados".

[221] STC 94/1998 de 4 de mayo (Sala segunda), FJ 4º.

El artículo 67, de actuaciones previas de investigación, utiliza el término tráfico como uno de los tratamientos de datos sometidos al Reglamento (UE) 2016/679, de tal forma estipula que se deba actuar para evitar un tráfico masivo de datos personales. Atribuye esta iniciativa a la Agencia Española de Protección de Datos, dándole potestad para la investigación de determinados tratamientos que impliquen un eventual tráfico masivo.

5.3.2.11. Transferencia y transmisión internacional

La RAE define transferencia como acción y efecto de transferir. También la RAE entiende por transferir pasar o llevar algo desde un lugar a otro.

La RAE define como transmisión como la acción o efectos de transmitir. También la RAE entiende por transmitir la acción de trasladar o transferir.

El Reglamento (UE) 2016/679 en el artículo 13, sobre información que deberá facilitarse cuando los datos personales se obtengan del interesado, y en el artículo 14, sobre información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado, se hace referencia a transferir datos personales a un tercer país u organización internacional como condición que obliga al responsable a informar a la persona titular de los datos.

El Reglamento (UE) 2016/679 se hace referencia a transferir datos personales a un tercer país u organización internacional como condición que obliga al responsable a informar a la persona titular de los datos.

La Ley Orgánica 3/2018 utiliza la expresión transferencia internacional de datos en varios de sus preceptos. El artículo 40, sobre el régimen de las transferencias internacionales de datos, incluye a la transferencia internacional de datos dentro de los tratamientos de datos regulados por el RGPD.

La Ley Orgánica 3/2018, en su artículo 42, sobre supuestos sometidos a autorización previa de las autoridades de protección de datos, distingue dos tipos de operaciones en el tratamiento de las transferencias internacionales de datos, aquellas dirigidas a países u organizaciones internacionales que cuenten con decisión de adecuación aprobada por la Comisión o que se amparen en alguna de las garantías previstas en el artículo anterior 41, y en el artículo 46.2 del Reglamento (UE) 2016/679 y los otros países que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos.

La Ley Orgánica 3/2018 en su artículo 43 (Supuestos sometidos a información previa a la autoridad de protección de datos competente) introduce otra operación necesaria dentro del tratamiento de las trasferencias de datos internacionales, esta es, la información previa a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos.

5.3.3. Elementos adicionales en el tratamiento de datos

A la definición completa de tratamiento de datos también se incluye la determinación de los elementos adicionales al tratamiento de datos. Debiéndose entender como elementos adicionales las acciones u operaciones no básicas ni complementarias que se deben realizar o pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley Orgánica 3/2018 o en alguno de ellos.

Como elementos adicionales en el tratamiento de datos personales se hacen constar las siguientes acciones o procesos: de automatización; de confidencialidad y de consentimiento; y de oposición.

5.3.3.1. Automatización

Automatización, en base a las fuentes consultadas, se considera genéricamente como el acto y la consecuencia de automatizar. Entendiendo por automatizar hacer algo o a algún proceso automático o indeliberado, utilizando no literalmente la definición de automatizar de la RAE. En el marco del tratamiento de datos, se entiende por automatización precisamente el proceso no manual del tratamiento de los datos en cualquiera de las fases del mismo.

El Reglamento (UE) hace mención al concepto de automatización, procedimientos automatizados, concretamente en la propia definición de tratamiento que expone en su artículo 4 a efectos del Reglamento (UE). Así pues, dicho artículo define al tratamiento de datos como aquella operación o conjunto de operaciones realizadas sobre datos por cualquier procedimiento, automatizados o no automatizado.

La Ley Orgánica 3/2018, hace una mención especial al término automatizado. Esta Ley Orgánica en su artículo 2, del ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94, explica que el término dato personal implica a "datos personales contenidos o destinados a ser incluidos en un fichero" independientemente del método que se utilice para su tratamiento, incluyendo el informático y el no informático, automatizado o manual.

En otras palabras, el proceso de automatización será el que permita pasar del proceso manual al proceso automatizado, en principio se puede entender como pasar de un tratamiento del dato de forma manual, en principio en papel, a otro tratamiento automatizado, como no puede ser de otra forma, en soporte informático. También puede entenderse que el dato en soporte papel se traspone a un soporte informático para que pueda ser tratado automáticamente, aunque no obligatoriamente, dado que un dato en soporte informático también puede ser tratado manualmente.

5.3.3.2. Confidencialidad y consentimiento

Por confidencialidad, la RAE define la cualidad de confidencial. En este orden de cosas la RAE entiende por confidencial algo que se atribuye a cualquier dato personal que no pueda ser comunicado ni divulgado a tercero.

Por consentimiento, la RAE define como la acción o efecto de consentir; manifestación de voluntad, expresa o tácita, por la cual un sujeto se vincula jurídicamente.

El Reglamento (UE) 2016/679 entiende a la confidencialidad no como un elemento del tratamiento sino como un principio que debe atender y respetar el tratamiento de los datos en todas sus formas y expresiones. Así pues, el tratamiento se realizará confidencialmente, sin revelar identidad, o en confidencialidad, sin divulgación.

El artículo 28, sobre el encargado del tratamiento, introduce el concepto de "obligación de confidencialidad" en el contrato que deberá regir entre el responsable y el encargado este deberá hacer constas la obligación de confidencialidad tal como el artículo 28 describe en este contexto: "garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria".

El artículo 32.1, sobre seguridad del tratamiento, vuelve a insistir en que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: "b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento."

El artículo 39, sobre las funciones del delegado de protección de datos, establece que el delegado de protección de datos no tan solo deberá atender a un tratamiento de datos sometidos a criterios de confidencialidad, sino que él mismo tendrá la obligación que impone el secreto profesional, equiparando el mismo artículo dicha obligación a la confidencialidad.

El artículo 76, de la confidencialidad, se refiere a la confidencialidad al tratar en la Sección 3 sobre el Comité Europeo de Protección de Datos. En este aspecto obliga al Comité a organizar sus debates y los temas que contenga sus sesiones de trabajo bajo garantías de confidencialidad cuando así se considere necesario.

En cuanto a la Ley Orgánica 3/2018 entiende el término confidencialidad como un deber, cuyo sujeto es el responsable y/o encargado del tratamiento de datos personales. El artículo 5, del deber de confidencialidad, establece que el deber de confidencialidad afectará durante el tratamiento de datos tanto al responsable, como al encargado y como a toda persona que intervenga, en cualquiera de sus procesos o elementos. Este artículo 5 hace una remisión al artículo 5.1.f) del Reglamento (UE) 2016/679.

El artículo 9, de las categorías especiales de datos, utiliza el término confidencialidad como un requisito para el tratamiento de datos personales de los que se incluyen en el artículo 9, del tratamiento de categorías especiales de datos personales, del Reglamento 2016/679.

El artículo 24, sobre sistemas de información de denuncias internas, también utiliza el término confidencialidad para insistir en medios de seguridad para los datos de las personas de los sistemas de información de denuncias internas, en el siguiente literal

"Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas ".

El artículo 36, sobre la posición del delegado de protección de datos, de la Ley Orgánica 3/1028 vuelve sobre los pasos del artículo 39, de las funciones del delegado de protección de datos, del Reglamento (UE), en cuanto a los deberes del delegado de protección de datos, en este caso se pone de manifiesto que ni el responsable ni el encargado podrán oponerse a este deber que deberá tener presente el delegado, lo cual refuerza el posicionamiento de independencia de este.

La normativa relativa a protección de datos, tanto el Reglamento (UE) 2016/679 como la Ley Orgánica 3/2018, le dan al concepto de consentimiento una extraordinaria relevancia, convirtiéndolo en uno de sus elementos de mejora sobre la normativa derogada. La confidencialidad, más que una parte del tratamiento es en realidad una premisa para poder realizar el tratamiento de datos personales de acuerdo a la normativa que lo regula. En todo caso la normativa establece que el consentimiento es una de las vías posibles para la licitud del tratamiento de datos personales.

En cuanto al Reglamento (UE) 2016/679 el artículo 4, definiciones, define al consentimiento en los siguientes términos: "11) consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

Así pues, el consentimiento debe ser dado libremente, informadamente, específicamente e inequívocamente. En este sentido, un consentimiento libre, se ha expresado al AEPD en su comunicado del día 30 de abril de 2020 al decir:

> "Las personas afectadas no pueden negarse a someterse a la toma de temperatura sin perder, al mismo tiempo, la posibilidad de entrar en unos centros de trabajo, educativos o comerciales, o en los medios de transporte, a los que están interesados en acceder. Por tanto, ese consentimiento no sería libre, uno de los requisitos necesarios para invocar esta base legitimadora."

El artículo 6.1, sobre licitud del tratamiento, coloca al consentimiento como un requisito previo al tratamiento para aceptarlo como tratamiento licito. Lo expresa de la siguiente manera:

> "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. Si bien es cierto que el Reglamento (EU) determina que hay otras condiciones distintas al consentimiento para la licitud del tratamiento de datos personales".

El artículo 7, sobre las condiciones para el consentimiento, del Reglamento (UE) 2016/679, dedica todo su contenido al requisito del consentimiento. En este orden de cosas exige que el consentimiento deberá ser siempre demostrable, recae sobre el responsable del tratamiento demostrar que el interesado dio su consentimiento; deberá

ser para un único asunto; deberá ser posible su retirada; y el tratamiento se supeditará siempre al consentimiento.

El artículo 8, sobre condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, del Reglamento (UE) 2016/679, dedica su texto a la edad mínima de una persona para considerar válido su consentimiento en el ámbito de las tecnologías de la comunicación. En este sentido, en los servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. En España, el artículo 7.1 de la Ley Orgánica 3/2018, establece una edad límite superior a 14 años.

El Reglamento (UE) 2016/679 limita el poder del consentimiento y le quita el valor de absoluto. En el artículo 9, del tratamiento de categorías especiales de datos personales, determina que será lícito el tratamiento de datos "prohibidos" tales como los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física, cuando el interesado haya dado consentimiento explícito para el tratamiento de dichos datos personales, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición no puede ser levantada por el interesado.

El consentimiento de la persona o interesado no capacitado, física o jurídicamente, para dar su consentimiento no tendrá validez.

El artículo 6, sobre el tratamiento basado en el consentimiento del afectado, de la Ley Orgánica 3/2018 define el consentimiento utilizando el artículo 4.11 del Reglamento (UE) 2016/679.

El artículo 7 de la Ley Orgánica 3/2018, sobre el consentimiento de los menores de edad, en consonancia con el Reglamento (UE) 2016/679 en su artículo 8, de las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, determina la edad de quince años, mayor de catorce años, a partir de la cual sea suficiente su consentimiento, exceptuando los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

El artículo 9, sobre las categorías especiales de datos, del Reglamento (UE) 2016/679, estipula que el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, a los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, sin menos cabo del tratamiento al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679.

El artículo 9, continúa diciendo que los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad. En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

5.3.3.3. Oposición

Por oposición, la RAE entiende la acción o efecto de oponer u oponerse; entendiendo por oponer la acción de poner algo contra otra cosa para entorpecer o impedir su efecto; dicho de una cosa: ser contraria.

En cuanto al término oposición, el Reglamento (UE) trata a este término en el contexto del derecho de oposición, artículo 21.

La Ley Orgánica 3/2018, trata el término oposición en el contexto de los derechos subjetivos de la persona, así el artículo 12, sobre disposiciones generales sobre ejercicio de los derechos, y el artículo 18, del derecho de oposición.

Concluyendo, la acción u operación que hace efectiva la voluntad de oponerse conlleva un tratamiento del dato encaminado a cumplir tal efecto, es decir, la limitación al acceso o al tratamiento general de un dato o la oposición a cualquier tratamiento de un dato conlleva en sí mismo un tratamiento específico encaminado a tal objetivo.

5.4. Tratamiento de categorías especiales en Reglamento 2016/679 y Ley Orgánica 3/2018

En el contexto del Reglamento (UE) y de la Ley Orgánica 3/2018, hablar de tratamiento de datos es referirse a los elementos básicos del tratamiento de datos, a los elementos complementarios del tratamiento y a los elementos adicionales en el tratamiento de datos personales.

En este orden de cosas, los elementos básicos del tratamiento de datos que como ya se ha visto en el capítulo 5.3.1 del Título I, son todas las operaciones directas sobre datos que se pueden producir sobre los datos personales y que requieren de protección por parte del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 y que aparecen en el punto 2 del artículo 4, definiciones, del Reglamento (UE) 2016/679. Los elementos básicos contemplan las siguientes operaciones: acceso; adaptación y modificación; conservación; comunicación y difusión; cotejo; destrucción; extracción, consulta y utilización; interconexión; organización y estructuración; recogida y registro de datos; y supresión.

En relación a los elementos complementarios del tratamiento vistos en el capítulo 5.3.2. del Título I, estos son todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4, definiciones, del Reglamento (UE) 2016/679, en el punto relativo a tratamiento, pero que o son acciones u operaciones previas al tratamiento de los datos personales o son colaterales al tratamiento de datos y, a su vez, son necesarias

para que este tratamiento sea lícito y cumpla los principios de la norma o los derechos que ella proclama. Los elementos básicos contemplan las siguientes acciones: anonimización y seudonimización; bloqueo; circulación y portabilidad; mantenimiento; minimización; exactitud de datos; rectificación; reidentificación; reutilización; tráfico; y transferencia y transmisión internacional.

A estas dos categorías de elementos del tratamiento también se suman los elementos adicionales en el tratamiento de datos personales y que como consta en el capítulo 5.3.3 del Título I, son las acciones u operaciones no básicas ni complementarias que se deben realizar o pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley Orgánica 3/2018 o en alguno de ellos. Como elementos adicionales en el tratamiento de datos personales se hacen constar la: automatización; confidencialidad y consentimiento; y limitación y oposición.

De tal forma que se aplicarán todos estos elementos, básicos, complementarios y adicionales, a las categorías especiales de datos del Reglamento (UE) 2016/679 y Ley Orgánica 3/2018.

En otro orden de cosas, como ya se ha comentado en el capítulo 1.7, sobre categorías especiales de datos, del Título I y en especial en el capítulo 1.7.5, del listado de los datos de categoría especial, en cada norma y su análisis comparativo, del Título I, el Reglamento (UE) 2016/679 no despliega ninguno de sus artículos como categoría especial de datos, sino que directamente en su artículo 9 el Reglamento (UE) 2016/679 utiliza la expresión tratamiento de categorías especiales de datos personales.

La Ley Orgánica 3/2018, si introduce en su articulado “las categorías especiales de datos” concretamente en si artículo 9. Sin embargo, el artículo 9 de la Ley Orgánica 3/2018 se remite a lo que dice el artículo 9 del Reglamento (UE) 2016/679.

Una de las razones posibles para justificar esta decisión que toma el legislador a través del Reglamento (UE) es que el reglamento se basa en la regulación del tratamiento de los datos personales y no en la clasificación de los datos, en realidad, los determina pasivamente.

La acción del Reglamento (U)E entiende que el tratamiento de datos no es lícito y que solo será licito si cumple lo estipulado en el artículo 6, sobre licitud del tratamiento, exponiendo en su punto 1 que “El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones”. Así pues, el Reglamento (UE) 2016/679 crea las condiciones de licitud del tratamiento de datos.

Las **condiciones de licitud** (base jurídica) se clasifican en las siguientes:

1. Por consentimiento
2. Por exigencia legal, por contrato o por ley
3. Por interés vitales de cualquier persona física
4. Por interés público
5. Por ejercicio de la autoridad pública
6. Por el interés legítimo del responsable del tratamiento

Así pues, el Reglamento (UE) no clasifica a los datos de forma explícita, sino que introduce unos tipos de datos que denomina de categoría especial y, en consecuencia, de facto, crea otro tipo de datos que incluye a "todo el otro dato que no sea categoría especial".

Esta clasificación la realiza mediante la prohibición de cualquier tratamiento de un listado de tipos especiales de datos vinculados con derechos fundamentales de las personas y que el artículo 9 lo expresa de la siguiente manera:

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

Dado que el Reglamento no clasifica los datos sino el tratamiento de los mismos, en el artículo 9 excluye de dicha prohibición determinadas circunstancias, es decir, siguen siendo datos de categoría especial pero que una circunstancia ajena permite su tratamiento sin el necesario consentimiento de la persona, es decir, determina que exista base jurídica para su tratamiento.

El propio Reglamento (UE) se autoimpone una serie de exclusiones de la prohibición del artículo 9, pero dentro del siguiente escenario:

- siempre, respetando en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
- siempre, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido;
- siempre, respetando en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Las exclusiones del artículo 9 se pueden clasificar en dos grandes grupos, por una parte, las circunstancias de exclusión que afectan a la persona física, afectado o tercero, y por otra parte, las circunstancias de exclusión ajenas a la persona interesada y que estas se dividen, a su vez, en situaciones atribuirles a funciones de potestad o al interés general o a otras situaciones. De esta forma se detallan en el siguiente listado la clasificación de las exclusiones que hace el artículo 9 de las prohibiciones de tratamiento:

1. Circunstancias que afectan a la persona física, afectado o tercero:
    a. Cuando el interesado haya hecho públicos sus datos personales.
    b. Cuando haya consentimiento. Sin embargo, no otorga al consentimiento un valor absoluto, dado que condiciona el consentimiento a que el ordenamiento jurídico del Estado no lo contradiga o cuando el interesado no esté

capacitado, física o jurídicamente, para dar su consentimiento y haya que proteger intereses vitales del interesado o de otra persona física.

c. Cuando es necesario para fines de relativos a la salud y sin perjuicio de las condiciones y garantías contempladas en el apartado 3.

2. Circunstancias ajenas a la persona afectada:
   a. atribuidas por funciones de potestad:
      i. Cuando se utilice para el ejercicio o la defensa de reclamaciones.
      ii. Cuando los tribunales actúen en ejercicio de su función judicial.
      iii. Cuando, en Derecho laboral y de la seguridad y protección social, haya cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado.
   b. afectadas por el interés general:
      i. Cuando prevalezca el interés público esencial, debe ser proporcional al objetivo perseguido.
      ii. Cuando es necesario por razones de la salud pública.
      iii. Cuando es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
   c. Otras
      i. El tratamiento de datos de los miembros, actuales o antiguos, de organismos sin ánimo de lucro políticos, filosóficos, religiosos o sindicales, o de personas que mantengan contactos regulares con ellos, en relación con sus fines. Siempre que los datos personales no se comuniquen fuera de estos sin el consentimiento de los interesados.

Todas estas exclusiones se podrán aplicar cuando sean realizadas por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, tal como se ve en el siguiente apartado.

En resumen, el tratamiento de los datos de categorías especiales del artículo 9 del Reglamento (UE) y del artículo 9 de la Ley Orgánica 3/2018, tendrá que estar a los elementos básicos, a los elementos complementarios y a los elementos adicionales sujetos a las condiciones de legitimidad del artículo y a la exención de prohibición del artículo 9, la cual está sujeta a la condición de secreto profesional.

5.5. Legitimación para el tratamiento de los datos. El secreto profesional

5.5.1. Tipos de legitimación en derecho

Las actuaciones de personas física y jurídicas tiene que atenerse a las normas de rango superior que las regulan, en su caso. Estas normas podrán poner sus límites a dicha actuaciones, prohibirlas, autorizarlas, excepcionarlas, controlarlas y sancionarlas, entre otras muchas acciones legales posibles en derecho. La sujeción a dichas exigencias en el

ordenamiento jurídico atiende al principio de legalidad, artículo 9 de la Constitución Española de 1978.

La capacidad de obrar como aptitud para celebrar actos jurídicos no basta por si misma para poder realizar válidamente todo tipo de actos. Hace falta además que al sujeto le sea posible realizar el acto concreto y singular frente al que está, a esto podemos denominarlo legitimación.

El estudio de la dogmática del derecho procesal es útil para centrar el significado de la legitimación. La teoría de las partes del proceso civil se presenta como un elemento fundamental para la obtención de una tutela judicial, la cual trata de la capacidad para ser parte, de la capacidad de obrar en un proceso y de la legitimación de las partes. Concretando, la legitimación en los procesos se clasifica como legitimación activa y legitimación pasiva, en base a la posición del sujeto en el proceso, y de legitimación ordinaria y de legitimación extraordinaria, en base al origen del derecho que soporta la acción o la posición de cada parte[222].

La legitimación ordinaria es la que actúa en los titulares de la relación jurídica u objeto litigioso, artículo 10 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, se sustenta en la titularidad del derecho subjetivo o en la imputación de la obligación. Esta regla tiene una excepción, que por ley se atribuya legitimación a persona distinta del titular, artículo 10 y artículo 11 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en cuyo caso aparece la legitimidad extraordinaria.

En derecho procesal también se utiliza la expresión legitimación activa para determinar a la parte demandante y legitimación pasiva[223], a la parte demandada[224]. También se entiende que la legitimación puede ser directa e indirecta, la directa corresponde a la legitimación ordinaria y la indirecta a la legitimación extraordinaria [225].

En este orden de cosas, el derecho a través de la expresión legitimación designa a quien dispone de un derecho subjetivo o también a quien tiene un interés legítimo. A lo cual hay que añadir, "a diferencia de lo que sucede con los requisitos de capacidad, la legitimación debe ser tratada como una cuestión que afecta al fondo del asunto"[226].

Este capítulo 5.5 del Título I, evidentemente no tiene su fin en el derecho procesal, pero utiliza la teoría del derecho procesal de la legitimación como base teórica para explicar legitimidad en el tratamiento de datos del RGPD y su relación con la licitud del tratamiento de datos personales dentro del Reglamento (UE) 2016/679.

En este proceso de analogía se sitúa a la persona titular de los datos como la parte titular del derecho subjetivo de tratar sus datos personales, es decir, de entrada, el RGPD

[222] ROBLES GARZÓN, J.A. (2013) "Conceptos básicos de derecho procesal civil" Madrid. Editorial Tecnos, Grupo Anaya. pp 193-200.

[223] ROBLES GARZÓN, J.A. (2013) "Conceptos básicos …..", op.cit; p 199.

[224] STS 713/2007, de 27 de junio de 2007 (Sala Primera de lo Civil), FJ 2º.

[225] ROBLES GARZÓN, J.A. (2013) "Conceptos básicos …..", op.cit; p 200.

[226] DAMIÁN MORENO J. (2016) "Lección. Tener o no tener legitimación. De eso se trata". Derecho procesal. 12 diciembre de 2016. Disponible en www.almacendelderecho.org. (28/02/2021).

entiende que la única parte que puede disponer libremente de sus datos es la persona interesada, aunque también está libre disposición tiene sus límites en cuanto se manifieste a través del consentimiento.

Así mismo, la persona titular del derecho subjetivo sobre sus datos es a través del consentimiento regulado por el artículo 7 y en el artículo 8, en el caso de niños, que puede levantar la ilicitud del tratamiento de sus datos personales por terceras personas, aunque con limitaciones. Sin embargo, esta ilicitud también puede ser levantada por distintos supuestos y situaciones jurídico-legales impuestas por la situación.

No obstante, el RGPD entiende que en determinadas situaciones en las cuales el dato a tratar sea considerado especial en su categoría, no es suficiente con que se haya levantado la prohibición mediante el consentimiento o mediante supuestos externos a la persona titular, sino que, además, la persona que vaya a tratar los datos especiales deberá gozar de una característica determinada que en función de las bases jurídicas del RGPD legitimará el tratamiento que realice sobre dichos datos.

Así pues, en base a la argumentación mantenida se entenderá que estas terceras personas podrán tratar datos, de categorías especiales, pertenecientes a la que es titular de los mismos, bien a través de la cesión del derecho subjetivo del titular del dato a esta tercera persona, que no es titular del dato, mediante la acción del consentimiento explicito o manifestación de la voluntad explícita y concreta, bien en otros dos supuestos. En uno de ellos, esta tercera persona podrá utilizar una cosa que el derecho asigna a otra persona, si esta persona cumple el requisito del secreto profesional, artículo 9.3 del RGPD, y en otros casos, cuando esta tercera persona es la Autoridad de control o el delegado de protección de datos, ambos por el secreto profesional.

5.5.2. La legitimación en el Reglamento (UE) 2016/679

"El Reglamento (UE) 2016/679 mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime."[227]

La clasificación tradicional de legitimación aplicada al contexto del Reglamento (UE) 2016/679 induce la existencia de dos tipos de legitimación, la de legitimación subjetiva y legitimación objetiva. La legitimación subjetiva fundamentada en el derecho subjetivo de la parte y la legitimación objetiva fundamentada en las excepciones que la ley impone a la ilicitud del tratamiento de los datos de cualquier persona.

La tradicional legitimación ordinaria aplicada al RGPD vendría a mostrase como la legitimación subjetiva, siendo directa cuando la parte es el titular de los datos.

La legitimación para el tratamiento de datos que concede el RGPD a determinadas situaciones jurídico-legales que superan la protección del tratamiento del dato personal, ubicadas en el capítulo 6, se entienden como lo que la legitimación tradicional entiende

[227] AEPD (2019) "Guía del Reglamento General de Protección de Datos. Para responsables del tratamiento". Guía de protección de datos UE. Septiembre 2019.Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf (31/01/2021).

como legitimación extraordinaria. Al igual ocurre con los supuestos que el artículo 9.2 expone para levantar la prohibición del tratamiento del dato de categorías espaciales.

La legitimación extraordinaria aplicada a RGPD se mostraría como una legitimación subjetiva indirecta cuando el RGPD concede la legitimación que, a terceras personas por su naturaleza o dedicación, tal es el caso de la personal sometida a secreto profesional o los poderes que el artículo 58 concede a la Autoridad de control.

El Reglamento (UE) a través de su artículo 6, prohíbe el tratamiento de datos personales y es el propio artículo 6 el que establece los requisitos para que el tratamiento de estos datos sea lítico, es decir, legitima a terceras personas distintas al titular de los datos para el tratamiento a través de un listado de supuestos que constituyen la base jurídica del tratamiento. Una condición de licitud es la que la ley otorga al titular del dato protegido, el consentimiento, mientras que otros requisitos vienen impuestos por la situación o consideración jurídico-legal, externas el sujeto titular y amparadas por el ordenamiento jurídico, de la circunstancia que rodea o condiciona a la persona titular y que levanta la ilicitud del artículo 6 o la prohibición del artículo 9.2. Siguiendo con esta última línea de argumentación, entendemos que cabe otro tipo de legitimación extraordinaria en el RGPD, esta es la por legitimación objetiva.

Así pues, el artículo 5.1.a) del RGPD obliga a que el tratamiento de datos llevado a cabo por un tercero distinto del titular de los datos, sea siempre lítico y este lo será cuanto cumpla el artículo 6 y el artículo 9 del RGPD. En este orden de cosas, se entenderá por legitimación objetiva del RGPD como aquella legitimación sustentada en la situación ajena al titular, amparada por el ordenamiento jurídico, que levanta la ilicitud del artículo 6 o la prohibición del artículo 9.2.

Como base jurídica de legitimación a un tercero para el tratamiento de datos aparece en primer lugar el consentimiento del interesado, la manifestación de su libre voluntad. Es decir, apela al derecho subjetivo de la persona de determinar libremente cuando quiere que un dato suyo sea tratado. A esta causa de licitud o de legitimación la hemos denominamos legitimación subjetiva directa.

Tabla 4. Tipos de legitimación en el RGPD (elaboración propia)

Tradicional	Reglamento (UE) 2016/679	
Legimimación ordinaria	Legimitación subjetiva	Legimitación subjetiva directa
Legimimación exordinaria	Legimitación subjetiva	Legimitación subjetiva indirecta
	Legimitación objetiva	

El RGPD levanta la ilicitud en unos casos y desactiva la prohibición del tratamiento en determinados supuestos vinculados con la naturaleza de una tercera persona, esto

ocurre en dos casos, por una parte, en el caso de la tercera persona sometida al secreto profesional y, por otra parte, en el caso de la persona que ostente la Autoridad de control. En estos supuestos entendemos que la legitimación es una legitimación subjetiva indirecta, en realidad una legitimación subjetiva a terceros.

La legalidad exigida en base al principio de legalidad puede entenderse desde un prisma pasivo y desde un prisma activo. Entendemos que el prisma es pasivo, desde el punto de vista del dato, es decir, el dato que va a ser tratado. Entendemos que el prisma es activo, desde un punto de la persona, es decir, la persona que los va a tratar. Un dato podrá o no estar sujeto al RGPD y la persona que trate el dato podrá o no estar autorizada a hacerlo.

Este apartado, sobre las bases jurídicas para el tratamiento de datos dentro del Reglamento (UE) 2016/679, se fundamenta desde un punto de vista activo, es decir, la causa legitimadora que autoriza a una persona tratar datos de otra persona.

Será licito el tratamiento de los datos, en primer lugar, cuando lo realice la figura del responsable, en segundo lugar, la figura del encargado, en tercer lugar, la figura del delegado de la protección de datos y en cuarto lugar, cuando lo realice aquella persona que cumplimento los requisitos de seguridad que impone la norma cumpla las condiciones de legitimación del artículo 6.1 del Reglamento (UE) 2016/679 y cuando se trata de categorías especiales de datos, además, por el artículo 9.2 del Reglamento (UE) 2016/679.

Tal como ya se ha visto en el punto 4 de este mismo capítulo 5, las condiciones de licitud requeridas para un tratamiento de datos son las que contempla el artículo 6.1 del Reglamento (UE) 2016/679. Las **condiciones de licitud** o bases jurídicas o causas de legitimación de un tercero, se clasifican en las siguientes[228], previstas legalmente en el artículo 6.1 RGPD:

1. Por consentimiento
2. Por exigencia legal, por contrato o por ley
3. Por interés vitales de cualquier persona física
4. Por interés público
5. Por ejercicio de la autoridad pública
6. Por el interés legítimo del responsable del tratamiento

La legitimidad vendrá dada tanto por el cumplimiento de las condiciones de licitud como por la observancia de los principios relativos al tratamiento del artículo 5 del Reglamento (UE) 2016/679 y los principios de protección de datos del Título II de la Ley Orgánica 2018.

Sin embargo, las condiciones de licitud y la observancia de los principios de la protección de datos no son suficientes en todos los casos que se pudieran dar. En este sentido, para el tratamiento de los datos de categorías especiales del artículo 9 del Reglamento (UE)

[228] GARCÍA PÉREZ, RM. (2020) "Bases jurídicas relevantes del tratamiento de datos personales en la contratación de contenidos y servicios digitales" Cuadernos de Derecho Transnacional. Vol. 12, nº 1, 875-907.

2016/679 y del artículo 9 de la Ley Orgánica 3/2018, hace falta otro tipo adicional de legitimación. Concretamente, las bases jurídicas que parecen en el artículo 9.

El interés legítimo entra en juego en el proceso de legitimación. De esta forma el Considerando 47 del RGPD dice:

> "El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable."

Es el artículo 20.1 del Reglamento (UE) 2016/679 el que de una forma clara marca el límite del interés legítimo, de tal forma entiende que

> "El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones."

Finalmente hay que comentar que los Considerando 47 a 49 de RGPD recoge algunos ejemplos de intereses legítimos[229]:

- Prevención de fraude
- Marketing directo
- Trasmisiones de datos en grupos de empresas para fines administrativos internos
- Trasmisiones de datos para garantizar la seguridad de las redes y para impedir el acceso no autorizado a las redes de comunicaciones electrónicas

5.5.3. El secreto profesional. Legitimación subjetiva a terceros

En base al punto anterior, se ha concluido que la legitimación puede ser subjetiva directa, es decir, la que tiene la persona interesada. También tendrá base jurídica de licitud o base jurídica para la legitimación de otras personas o de terceras personas que sin el consentimiento del interesado puedan tratar sus datos e incluso en el supuesto de que el tratamiento prohibido este sometido a excepciones que inhiban la prohibición, siendo esta causa de licitud, el secreto profesional. En este supuesto, la Tesis propone hablar de legitimación subjetiva a terceros o legitimación subjetiva indirecta.

El Reglamento (UE) determina que tan solo determinadas personas o profesionales podrán tratar los datos personales acogiéndose al tratamiento de las categorías especiales de datos a que se refiere el apartado 2, letra h), los relativos a la salud. Estas

[229] LÓPEZ GARRIDO, L. (2018) "La protección de datos personales y el caso Facebook: una cuestión trasnacional". Revista Privacidad y Derecho Digital, 11, 147-173 Año III. pp 154-155.

personas legitimadas por las bases jurídica que apareen en el Reglamento (UE) para el tratamiento de los datos relativos a salud sin el consentimiento del interesado, son:

1. "los profesionales sujetos a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes
2. cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes"

Se entiende por secreto profesional la obligación que adquieren unos determinados profesionales de no desvelar ningún tipo de información que haya podido suministrale un cliente suyo. "No debe confundirse el deber de secreto con el secreto profesional al que están sometidas determinadas personas en función de la profesión que ejercen."[230]

Este deber de confidencialidad nace, por una parte, de los derechos fundamentales de las personas en relación con su intimidad y a su privacidad, y del derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales, y, de otra parte, de la propia naturaleza del servicio que recibe el cliente por parte del profesional y que, sin esta condición, confidencialidad, el servicio no sería posible llevarlo a cabo. Es decir, a persona se ve obligada a transmitir datos o información personal como requerimiento básico del servicio que demanda.

La naturaleza del servicio que obliga al deber de confidencialidad puede venir atribuida por preceptos legales de obligado cumplimiento, como es el caso de un abogado y su cliente o el caso de un paciente y su médico o cualquier profesión de la salud, como enfermería, psicología, farmacia, etc., en cuyo caso la atribución de confidencialidad viene comandada por la relación de la información suministrada con la protección de determinados derechos fundamentales de la persona como es el de la intimidad, Artículo 18 de la Constitución Española de 1978 y dignidad entre otras. El secreto profesional también se aplica a profesiones como los delegados de prevención de accidentes laborales, el trabajador social y los sacerdotes de confesiones religiosas y en alguna forma también se aplica al periodista, artículo 10 del Código Deontológico de la Federación de Asociaciones de Periodistas de España y artículo 19 de la Declaración Universal de Derechos Humanos[231].

La falta de definición legal del secreto profesional y concretamente sobre el criterio del Tribunal Superno de que "el secreto médico es una modalidad del secreto profesional" introduce ciertas limitaciones al secreto profesional de los profesionales de la medicina pues "los tribunales no han reconocido el secreto médico como un derecho subjetivo en

[230] MEDINACELI DÍAZ, K.I. (2016) "El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano", Tesis Doctoral. Facultad de Ciencias de la Educación, Universidad Pontificia Comillas. Madrid. España. p 168.

[231] PERIODISTAS EN ESPAÑOL.COM (27 noviembre 1993) "Código Deontológico de la Federación de Asociaciones de Periodistas de España (FAPE)". Disponible en https://periodistas-es.com/politica-editorial/codigo-deontologico-de-la-fapev (31/05/2020).

sentido estricto del médico y del paciente"[232], aunque también es cierto que la reforma del año 1995 a través de su artículo 199.2 , en su Título X, permite la inclusión del médico en el secreto profesional[233], a lo cual cabe añadir "la inclusión sin ningún género de duda del profesional de la medicina como uno de los posibles sujetos activos del mismo pone fin al vacío legal que existía"[234].

El deber de secreto profesional se extiende al ámbito de trabajo y relaciones laborales del profesional directamente implicado en el mismo, así, en el caso de los abogados[235], se extiende a los pasantes, procuradores, licenciados en derechos o meros estudiantes de derecho en prácticas y cualquier personal auxiliar con acceso a los datos del cliente.

Así pues, el secreto profesional se atribuye a una persona por ser profesional o por ejercer una profesión obligada a la confidencialidad de lo manifestado, comunicado o facilitado por su cliente o peticionario.

El ordenamiento jurídico también emana o da pie a la creación ex post de la figura del "secreto profesional sobrevenido". Este tipo secreto profesional ex post, es el que se atribuye a un profesional o trabajador que, por circunstancias de su trabajo o desempeño laboral y no por la circunstancia de su profesión, haya tenido acceso a ciertos documentos confidenciales de algún tipo de cliente o persona. De tal forma que la ley obliga a esta persona a guardar secreto de lo que ha oído, visto o leído, no por su profesión sino por haber tenido acceso o contacto con datos protegidos en el desempeño de sus funciones laborales. De tal forma que el personal de una empresa u organización de trabajo o el trabajador que accede a los datos especialmente protegidos de una persona en el ejercicio de sus funciones queda sujeto al deber de secreto.

Este tipo de secreto profesional sobrevenido hace extensivo el secreto a todos los datos protegidos por el Reglamento (UE) 2016/679 pues son el artículo 6 y 9 los que levantan esta ilicitud, pero no exime el secreto de los mismos, tan solo permite tratarlos. De esta forma Doña Karina Ingrid Medinaceli Díaz, en su Tesis Doctoral de 2016 hace constar en su página 168 "En cualquier fase de tratamiento, las personas que utilizan los datos de carácter personal están obligadas al secreto profesional, es decir, no pueden revelar la información a terceros."[236]

Todo lo cual nos lleva a traer a este documento una de las conclusiones de la Tesis Doctoral de Lucia Nicole Cristea Uivaru de 2017[237], que en su conclusión cuarta dice:

[232] SANCHEZ-CARO J., ABELLAN F. (2003) "Derechos y deberes de los pacientes", Granada, Ed. Comares. p 13

[233] REQUEJO NAVEROS MT. (2007) "El secreto profesional del médico y su protección jurídico penal: una perspectiva histórica". Foro, Nueva Época, 6, 159-194, p 185.

[234] REQUEJO NAVEROS MT. (2007) "El secreto profesional …..", op.cit; p 193.

[235] artículo 5 del Código Deontológico adoptado por el Estatuto General de la Abogacía Española, aprobado por Real Decreto 658/2001, de 22 de junio.

[236] MEDINACELI DÍAZ, K.I. (2016) "El tratamiento de los datos …..", op.cit; p 168.

[237] CRISTEA UIVARU, LN. (2017) "La protección de datos de carácter sensible en el ámbito europeo. Historia clínica digital y big data en salud". Tesis Doctoral. Facultad de Derecho, Universidad Abad Oliva, CEU, Barcelona, España. p 321.

> "En este sentido, creemos conveniente que además de la protección que reciben los titulares de los datos, los profesionales e intervinientes en los mimos, debería estar sujetos a una confidencialidad mucho más rigurosa y especifica al igual que el secreto médico hacia sus pacientes"

Este deber de secreto profesional sobrevenido se deriva de la siguiente legislación española vigente: el artículo 199 del Código Penal; en el artículo 127 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras; el artículo 10 de la Ley 14/1986; en el artículo 16.6 de La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; artículo 5 de la Ley 14/2007, de 3 de julio, de Investigación biomédica; y artículo 43 de la Ley 33/2011, de 4 de octubre, General de Salud Pública.

Ahora bien, el secreto profesional no es una cuestión absoluta o valor único. La fundamentación del secreto profesional se debe contraponer a la obligación de poner en conocimiento de la autoridad competente cualquier tipo de delito público, la cual tiene algunas excepciones aplicables solo a los abogados y a los sacerdotes.

Tienen obligación de secreto profesional en primer lugar los abogados y, en segundo lugar, los profesionales de la salud, los delegados de prevención de accidentes laborales, el trabajador social, los sacerdotes de confesiones religiosas y en alguna forma los periodistas. Pero, por otra parte, tienen la obligación de denunciar el conocimiento o notica sobre un acto delictivo o sobre algo que pueda serlo toda persona que por el cargo que ocupa tuviere noticas de acto que pudiera ser constitutivo de delito y tienen el deber de denunciar el que tuviere conocimiento o alguna notica de un delito.

A esta obligación del deber de denunciar se oponen una serie de exclusiones, por no tener el deber o la obligación de denunciar las noticias que tuvieran en conocimiento por medio del ejercicio de sus funciones. Estas exclusiones incluyen a: los menores de edad, los incapaces, los cónyuges no separados legalmente o con análoga relación de afectividad, los ascendientes y descendientes hasta segundo grado de parentesco, los abogados y procuradores por la información que reciban de sus clientes y los eclesiásticos y ministros de culto.

En este orden de cosas, en primer lugar, se describe la fundamentación del secreto profesional para luego pasar a la fundamentación de la obligación a la denuncia.

La fundamentación jurídica de secreto profesional con carácter general, en el sector de la abogacía y en el sector de la salud:

A) Con carácter general

   a. Constitución Española de 1978

      - Artículo 24 de la CE: "La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos".

b. Código Penal (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal)

- Artículo 199 del Código Penal:

> "1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.
>
> 2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años."

c. Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. En su capítulo V se trata del Deber de secreto profesional y uso de información confidencial.

- Artículo 127. Deber de secreto profesional. Dice:

> "1. Salvo los datos inscribibles en el registro administrativo al que se refiere el artículo 40, los datos, documentos e informaciones que obren en poder de la Dirección General de Seguros y Fondos de Pensiones en virtud de cuantas funciones le encomienda esta Ley tendrán carácter reservado.
>
> 2. Todas las personas que ejerzan o hayan ejercido una actividad de ordenación y supervisión de entidades aseguradoras y reaseguradoras, así como aquellas a quienes se les haya encomendado funciones respecto de dichas entidades, tendrán obligación de guardar secreto profesional sobre las informaciones confidenciales que reciban a título profesional en el ejercicio de tal función. ……."

B) En el ámbito del ejercicio de la abogacía

a. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial

- Artículo 542 de la Ley Orgánica del Poder Judicial, dice:

> "3. Los abogados deberán guardar secreto de todos los hechos o noticias de que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos."

b. Estatuto general de la abogacía (Real Decreto 658/2001, de 22 de junio, por el que se aprueba el Estatuto General de la Abogacía Española)

- Artículo 32:

> "1. De conformidad con lo establecido por el artículo 437.2 de la Ley Orgánica del Poder Judicial, los abogados deberán guardar secreto de todos los hechos o noticias que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos."

- Artículo 34:

> "Son deberes de los colegiados: e) Mantener como materia reservada las conversaciones y correspondencia habidas con el abogado o abogados contrarios,

con prohibición de revelarlos o presentarlos en juicio sin su previo consentimiento. No obstante, por causa grave, la Junta de Gobierno del Colegio podrá discrecionalmente autorizar su revelación o presentación en juicio sin dicho consentimiento previo."

- Artículo 42:

  "1. Son obligaciones del abogado para con la parte por él defendida, además de las que se deriven de sus relaciones contractuales, el cumplimiento de la misión de defensa que le sea encomendada con el máximo celo y diligencia y guardando el secreto profesional."

c. Código Deontológico de la Abogacía (aprobado por el Pleno del Consejo General de la Abogacía Española el 6 de marzo de 2019)[238]

- Artículo 5.- Secreto profesional:

  "1. La confianza y confidencialidad en las relaciones con el cliente, ínsita en el derecho de éste a su defensa e intimidad y a no declarar en su contra, impone a quien ejerce la Abogacía la obligación de guardar secreto, y, a la vez, le confiere este derecho, respecto de los hechos o noticias que conozca por razón de cualquiera de las modalidades de su actuación profesional, limitándose el uso de la información recibida del cliente a las necesidades de su defensa y asesoramiento o consejo jurídico, sin que pueda ser obligado a declarar sobre ellos como reconoce la Ley Orgánica del Poder Judicial.

  2. El deber y derecho al secreto profesional comprende todas las confidencias y propuestas del cliente, las de la parte adversa, las de los compañeros, así como todos los hechos y documentos de que haya tenido noticia o haya remitido o recibido por razón de cualquiera de las modalidades de su actuación profesional.

  3. Cualquier tipo de comunicación entre profesionales de la Abogacía, recibida o remitida, está amparada por el secreto profesional, no pudiendo ser facilitada al cliente ni aportada a los Tribunales ni utilizada en cualquier otro ámbito, salvo autorización expresa del remitente y del destinatario, o, en su defecto, de la Junta de Gobierno, que podrá autorizarlo discrecionalmente, por causa grave y previa resolución motivada con audiencia de los interesados. En caso de sustitución, esta prohibición le estará impuesta al sustituto respecto de la correspondencia que el sustituido haya mantenido con otros profesionales de la Abogacía, requiriéndose la autorización de todos los que hayan intervenido.

  Se exceptúan de esta prohibición las comunicaciones en las que el remitente deje expresa constancia de que no están sujetas al secreto profesional.

  4. Las conversaciones mantenidas con los clientes o con los contrarios, de presencia o por cualquier medio telefónico o telemático, en que intervengan profesionales de la Abogacía no podrán ser grabadas sin previa advertencia y conformidad de todos los intervinientes y siempre quedarán amparadas por el secreto profesional.

[238] CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA (6 marzo 2019) "Código Deontológico adoptado por el Estatuto General de la Abogacía Española". Disponible en https://www.abogacia.es/wp-content/ uploads/ 2019/05/Codigo-Deontologico-2019.pdf (31/05/2020).

5. El secreto profesional ampara las comunicaciones y negociaciones orales y escritas de todo tipo, con independencia del medio o soporte utilizado.

6. El deber de secreto profesional en relación con los asuntos profesionales encomendados, o en los que intervenga cualquiera de los miembros de un despacho colectivo, se extiende y vincula a todos y cada uno de ellos.

7. En todo caso, quien ejerce la Abogacía deberá hacer respetar el secreto profesional a cualquier otra persona que colabore con él en su actividad.

8. La obligación de guardar el secreto profesional permanece incluso después de haber cesado en la prestación de los servicios al cliente o abandonado el despacho donde se estaba incorporado, sin que esté limitada en el tiempo.

9. Solamente podrá hacerse uso de hechos o noticias sobre los cuales se deba guardar el secreto profesional cuando se utilice en el marco de una información previa, de un expediente disciplinario o para la propia defensa en un procedimiento de reclamación por responsabilidad penal, civil o deontológica. Todo ello sin perjuicio de lo dispuesto en relación con la aportación de la correspondencia habida con otros profesionales de la Abogacía en el número 3 de este artículo.

10. El consentimiento del cliente no excusa de la preservación del secreto profesional.

11. No se aceptará el encargo cuando se haya mantenido con la parte adversa una entrevista para evacuar una consulta referida al mismo asunto y ésta afecte a su deber de secreto profesional."

C) En el sector de la salud

a. La Ley 14/1986, General de Sanidad, de 25 de abril

- Artículo 10, dice:

"Todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias: 3. A la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público."

b. Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales

- Artículo 36. Competencias y facultades de los Delegados de Prevención, dice:

"2. En el ejercicio de las competencias atribuidas a los Delegados de Prevención, éstos estarán facultados para: b) Tener acceso, con las limitaciones previstas en el apartado 4 del artículo 22 de esta Ley, a la información y documentación relativa a las condiciones de trabajo que sean necesarias para el ejercicio de sus funciones y, en particular, a la prevista en los artículos 18 y 23 de esta Ley. Cuando la información esté sujeta a las limitaciones reseñadas, sólo podrá ser suministrada de manera que se garantice el respeto de la confidencialidad."

c. La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

- Artículos 7. El derecho a la intimidad (Capítulo III. Derecho a la intimidad), dice:

"1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes."

- Artículo 16. Usos de la historia clínica, dice: "1. La historia clínica es un instrumento (…)"

"3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

(…)

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso."

d. Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias. En el título I sobre el ejercicio de las profesiones sanitarias

- Artículo 8. Ejercicio profesional en las organizaciones sanitarias, dice en su punto 5:

> "En el supuesto de que, como consecuencia de la naturaleza jurídica de la relación en virtud de la cual se ejerza una profesión, el profesional hubiere de actuar en un asunto, forzosamente, conforme a criterios profesionales diferentes de los suyos, podrá hacerlo constar así por escrito, con la salvaguarda en todo caso del secreto profesional y sin menoscabo de la eficacia de su actuación y de los principios contenidos en los artículos 4 y 5 de esta ley."

e. Ley 14/2007, de 3 de julio, de Investigación biomédica

- Artículo 5. Protección de datos personales y garantías de confidencialidad, en su punto 4 dice:

> "Quedará sometida al deber de secreto cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico-asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación."

- Artículo 51. Deber de confidencialidad y derecho a la protección de los datos genéticos:

> "1. El personal que acceda a los datos genéticos en el ejercicio de sus funciones quedará sujeto al deber de secreto de forma permanente. Sólo con el consentimiento expreso y escrito de la persona de quien proceden se podrán revelar a terceros datos genéticos de carácter personal. Si no es posible publicar los resultados de una investigación sin identificar a los sujetos fuente, tales resultados sólo podrán ser publicados con su consentimiento."

f. La Ley 33/2011, de 4 de octubre, General de Salud Pública

- Artículo 43. Seguridad de la información, dice:

> "1. En todos los niveles del sistema de información en salud pública se adoptarán las medidas necesarias para garantizar la seguridad de los datos. 2. Los trabajadores de centros y servicios públicos y privados y quienes por razón de su actividad tengan acceso a los datos del sistema de información están obligadas a mantener secreto."

La fundamentación jurídica de la obligación a la denuncia y sus excepciones:

A) Ley de Enjuiciamiento Criminal (Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal)

- Artículo 262, dice:

> "Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio si se tratare de un delito flagrante.
>
> Los que no cumpliesen esta obligación incurrirán en la multa señalada en el artículo 259, que se impondrá disciplinariamente.

> Si la omisión en dar parte fuere de un Profesor en Medicina, Cirugía o Farmacia y tuviese relación con el ejercicio de sus actividades profesionales, la multa no podrá ser inferior a 125 pesetas ni superior a 250.
>
> Si el que hubiese incurrido en la omisión fuere empleado público, se pondrá además en conocimiento de su superior inmediato para los efectos a que hubiere lugar en el orden administrativo.
>
> Lo dispuesto en este artículo se entiende cuando la omisión no produjere responsabilidad con arreglo a las Leyes."

- Artículo 263:

> "La obligación impuesta en el párrafo primero del artículo anterior no comprenderá a los Abogados ni a los Procuradores respecto de las instrucciones o explicaciones que recibieren de sus clientes. Tampoco comprenderá a los eclesiásticos y ministros de cultos disidentes respecto de las noticias que se les hubieren revelado en el ejercicio de las funciones de su ministerio."

Resumiendo, la legitimación para tratar datos de personas se obtiene mediante las bases jurídicas de licitud y la observancia de los principios de la protección de datos y para el tratamiento de los datos de categorías especiales del artículo 9 del Reglamento (UE) 2016/679 y del artículo 9 de la Ley Orgánica 3/2018, hace falta además de cumplir con los eximentes de prohibición, otro tipo adicional de legitimación, el secreto profesional.

La existencia del secreto profesional sobrevenido, legitima a toda persona al tratamiento de los datos de las categorías especiales de los artículos 9, en el deber de guardar secreto.

Nota Crítica: el artículo 9 del Reglamento (UE) establece como bases jurídicas para la legitimación de una persona para el tratamiento de datos relativos a la salud o bien el consentimiento de la persona o bien la circunstancia de la obligación de guardar secreto descrita en alguna de las letras del artículo 9.2, permitiendo que el tratamiento pueda llevarse a cabo por una tercera persona. Por otra parte, la obligación de guardar secreto y en consecuencia el secreto profesional se hace extensiva a todos los datos protegidos por el Reglamento (UE) 2016/679 "En cualquier fase de tratamiento, las personas que utilizan los datos de carácter personal están obligadas al secreto profesional, es decir, no pueden revelar la información a terceros."[239] Se entiende que el secreto profesional y sobre todo el secreto profesional sobrevenido es un criterio o una circunstancia ambigua y demasiado general como para poder ser la que legitime el tratamiento de datos de tratamiento prohibido.

5.5.4. El interés legítimo del responsable del tratamiento en el RGPD

Antes de seguir adelante con este punto es de interés aclarar que no se debe confundir al interés legítimo con la base jurídica del interés legítimo.

[239] MEDINACELI DÍAZ, K.I. (2016) "El tratamiento de los datos …..", op.cit; p 168.

El interés legítimo debe ser aceptable en virtud de la ley[240]. El informe jurídico de la AEPD de 2019[241] entiende que

> "Una segunda posibilidad que excepciona la necesidad del consentimiento del interesado la constituye la existencia de un interés legítimo, siempre que en un ejercicio de ponderación entre dicho interés legítimo y los derechos fundamentales de los afectados prevaleciera el primero sobre el segundo"

El concepto de interés legítimo aplicado a la protección de datos apareció en la Directiva 95/46/CE, en su artículo 7.f). Esta directiva se trasladó al ordenamiento jurídico español mediante la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. El Tribunal Supremo en España planteó ante el Tribunal de Justicia de la Unión Europea una cuestión prejudicial, que a su vez venía derivada de dos procedimientos en los que había sido parte ASNEF y FECEMD, relativa a que el ordenamiento jurídico español establecía el requisito de que los datos estuviesen en fuentes de acceso público para poder aplicar la base legitimadora del interés legítimo. El Tribunal indica que se requiere una ponderación y considerar la lesión de los derechos fundamentales de la persona afectada por dicho tratamiento.[242]

El Tribunal de Justicia de la Unión Europea en mayo de 2014 se vuelve a pronunciar frente a la necesidad de la ponderación de los derechos e intereses de las personas afectadas por la aplicación de este criterio de licitud[243].

El interés legítimo es una condición que, cumpliéndose con los requisitos necesarios, es base jurídica para la licitud del tratamiento de los datos personales, tal como constan en el Considerando 47 del Reglamento (UE) 2016/679. Este Considerando dice:

> El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior.

[240] COMISIÓN EUROPEA (2014) "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". Adoptadas el 9 de abril de 2014. Grupo de trabajo sobre protección de datos del artículo 29. p 30.

[241] AEPD (2019) "Informe del Gabinete Jurídico sobre el Interés Legítimo". Septiembre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-interes-legitimo.pdf (28/02/2021).

[242] STJUE de 24 de noviembre de 2011 (C-468/10 y C-469/10), apartado 40 y 44.

[243] STJUE de 13 de mayo de 2014 (Gran sala) (asunto C-131/12), apartados 74, 76 y 86.

Este Considerando 47 excluye a la Administración pública de la utilización de la base jurídica del interés legítimo, de esta forma dice:

> Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

En resumen, en virtud de la jurisprudencia del TJUE de 2017[244] se requiere: 1) la existencia del interés legítimo, 2) que el tratamiento de los datos personales sea necesario para la satisfacción de dicho interés legítimo, y 3) que no prevalezcan los derechos y libertades fundamentales de los interesados.

5.6. Tratamiento de datos personales en la gestión de una epidemia-pandemia

La situación creada por la epidemia-pandemia del coronavirus en el mes de marzo de 2020 en España, durante la elaboración de esta Tesis doctoral, aconseja dedicar un espacio a las consecuencias de esta situación especial en el tratamiento de datos personales.

5.6.1. Concepto de alama de salud pública. Epidemia y pandemia

Cabe definir el concepto de epidemia y el de pandemia. Epidemia es definida por la RAE como "Enfermedad que se propaga durante algún tiempo por un país, acometiendo simultáneamente a gran número de personas". La ONG Médicos Sin Fronteras, define la epidemia "cuando una enfermedad contagiosa se propaga rápidamente en una población determinada, afectando simultáneamente a un gran número de personas durante un periodo de tiempo concreto"[245]. La Organización Mundial de la Salud llama pandemia a la propagación mundial de una nueva enfermedad.

Según la Fundación para el conocimiento Madrid, una epidemia es parte de la alerta epidemiológica en salud pública y en base al artículo publica en el blog de la Fundación[246] brote epidémico es:

1. "La aparición de dos o más casos de la misma enfermedad asociados en tiempo, lugar y persona.
2. El incremento significativo de casos en relación a los valores habitualmente observados.

[244] STJUE de 24 de mayo de 2017 (Sala Segunda) (C-13/16), apartado 28.

[245] MEDICOS SIN FRONTERAS. "Epidemias". Disponible en https://www.msf.es/nuestra-accion/ epidemias (28/02/2021).

[246] IBÁÑEZ MARTÍ, C. (27 febrero 2007) "Qué es un brote epidémico". Fundación para el conocimiento Madrid. Blog. Disponible en http://www.madrimasd.org/blogs/salud_ publica /2007/02/28/ 60163. (31/05/2020).

3. La agregación de casos de una enfermedad en un territorio y en un tiempo comprendido entre el mínimo y el máximo período de incubación o de latencia puede ser considerado, también, indicativo de brote.
4. La aparición de una enfermedad, problema o riesgo para la salud en una zona hasta entonces libre de ella.
5. La presencia de cualquier proceso relevante de intoxicación aguda colectiva, imputable a causa accidental, manipulación o consumo.
6. La aparición de cualquier incidencia de tipo catastrófico que afecte, o pueda afectar, a la salud de la Comunidad."

La bibliografía científica habla de epidemia o de brote indistintamente, refiriéndose a epidemia cuando existe un aumento inusual del número de casos de una determinada enfermedad en una población específica, en un periodo de tiempo determinado[247]. Otra bibliografía distingue brote como la aparición repentina de una enfermedad debida a una infección en un lugar específico y en un momento determinado, mientras que epidemia la define como un brote descontrolado y mantenido en el tiempo[248].

Por pandemia la RAE entiende a una enfermedad epidémica que se extiende a muchos países o que ataca a casi todos los individuos de una localidad o región. Para la OMS la pandemia es la propagación mundial de una nueva enfermedad, de tal forma que se produce una pandemia cuando surge un nuevo virus que se propaga por el mundo y la mayoría de las personas no tienen inmunidad contra él[249].

Otros expertos se refieren a una epidemia cuando existe en un periodo de tiempo determinado un aumento inusual del número de casos de una determinada enfermedad en una población específica[250]. Otros autores distinguen entre brote y epidemia, dándose esta última cuando un brote se mantiene en el tiempo, sin control [251].

Cuando una epidemia afecta a varios países entonces se habla de pandemia, según OMS[252]. Pero, en cualquier caso, estamos hablando de enfermedades transmisibles, infecciosas, de gran propagación y con afectación a varios continentes. Este es el caso que ocurrió el 11 de marzo de 2020 a raíz de la enfermedad producida por el SARS-Cov-2 afectando a más de 128.000 personas, en 114 países y con más de 4.290 muertes y

[247] HORCAJADA P., PADILLA, B. (2013) "Endemia y epidemia. Investigación de un brote epidémico nosocomial". Enfermedades Infecciosas y Microbiología Clínica, 31(3), 181-186, pp 181-186.

[248] PULIDO, S. (12 marzo 2020) "¿Cuál es la diferencia entre brote, epidemia y pandemia?". Gaceta sanitaria. Disponible en https://gacetamedica.com/investigacion/cual-es-la-diferencia-entre-brote-epidemia-y-pandemia/ (28/02/2021).

[249] OMS. Organización Mundial de la Salud (24 febrero 2010) "¿Qué es una pandemia?". Disponible https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/es/ (28/10/2021).

[250] HORCAJADA P., PADILLA, B. (2013) "Endemia y epidemia. Investigación …..", op.cit; pp 181-186.

[251] PULIDO, S. (12 marzo 2020) "¿Cuál es la diferencia …..", op.cit;

[252]OMS. Organización Mundial de la Salud "¿Qué es una pandemia?". 24 febrero 2010. Disponible en https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/es/ (28/02/2021).

que provocó que la Organización Mundial de la Salud clasificara dicha situación como una pandemia[253].

Las epidemias y por descontado las pandemias, son situaciones que deben ser controladas activamente desde su inicio o desde su sospecha, pues su propagación descontrolada puede acusar miles de muertes y millones de afectados. Tal como ha ocurrido durante loas años 2020 y 2021 con la pandemia COVID-19.

Las pandemias pueden causar múltiples víctimas, tal es el caso de las pandemias en el siglo XX como la pandemia de la gripe A del virus H_1N_1en 2009, llamada en un principio "gripe porcina" con 600.000 muertes; la pandemia del virus VIH iniciada en el año 1981, denominada la pandemia del SIDA, con más de 32 millones de muertes; la pandemia del virus Influenza A subtipo H_2N_2, conocida como la gripe "asiática" en el año 1957, con un millón de muertes; la pandemia del virus Influenza A subtipo H_3N_2,conocida como la gripe de "Hong Kong" en el año 1968, con un millón de muertes; la pandemia del virus Influenza A del subtipo H_1N_1 en el año 1918, llamada Gripe española, produjo más de 20 millones de muertes[254].

A fecha de 28 de octubre de 2020, después de que la OMS declarara la pandemia el día 11 de marzo, en el mundo, a las 19:10h (hora de Madrid), se registran 118.222.254 44.229.969 infectados detectados y 2.623.286 1.170.283 muertes. A fecha de 11 de marzo de 2021, en el mundo, a las 19:10h (hora de Madrid), se registran 118.222.254 infectados detectados y 2.623.286 muertes (Fuente: Johns Hopkins University) [255]. En un plazo de 134 días, en algo más de cuatro meses, la ratio mundial de afectados por cada diez mil habitantes ha pasado de 57,4 a 153,5 y el de muertes por diez mil habitantes ha pasado de 1,51 a 3,4.

En este orden de cosas, las ratios pandémicos más básicos y globalmente representativos son, por una parte, el número de infectados detectados por millón de habitantes, por otra parte, el número de muertes por millón de habitantes y el tanto por ciento de infectados que fallecen. Cada uno de ellos muestra una realidad distinta. Es muy importante tener en cuenta a la hora de comparar situaciones en distintos países y de esta forma calibrar magnitudes, que se debe relacionar las cifras de afectados y muertes, número de infectados o número de fallecidos, con la población total del país. Nada tiene que ver por ejemplo las cifras en términos absolutos de la Indica, China o USA con las de España o Francia y estas con las de Jamaica o Andorra.

[253]OPS. (11 marzo 2020) "La OMS caracteriza a COVID-19 como una pandemia". Organización Panamericana de la Salud. OMS. Disponible en https://www.paho.org/hq/index.php?option= com_ content&view= article&id= 15756: who-characterizes-covid-19-as-a-pandemic&Itemid= 1926&163ang =es (28/02/2021).

[254] BBC. Mundo.com "Coronavirus: las pandemias que pusieron al mundo en alerta en la historia reciente (y cómo se afrontaron)". Disponible en https://www.bbc.com/mundo/noticias-51843449 (28/02/2021).

[255] JOHNS HOPKINS UNIVERSITY Johns Hopkins University (28 octubre 2020) "COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE)" at Johns Hopkins University. Disponible en https://www.arcgis.com /apps/ opsdashboard/ index.html#/ bda7594740fd40299423467b48e9ecf6 (28/10/2020).

5.6.2. La salud pública en el orden internacional

Las enfermedades transmisibles no respetan las fronteras entre países por lo cual los países tienden a confiar en los criterios de los organismos supranacionales, internacionales, creados para el apoyo y control de enfermedades transmisibles.

En primer lugar, cabe nombrar a la Organización Mundial de la Salud (en adelante también OMS). La Organización de las Naciones Unidas (ONU) creó el 7 de abril de 1948 (Día Mundial de la Salud) a la OMS, como agencia internacional para la gestión de políticas de prevención, promoción y acciones sobre el terreno en cualquier lugar del mundo, para lo cual dispone de más de siete mil empleados, tiene oficinas en ciento cincuenta países y seis oficinas regionales. La sede de la OMS está en Ginebra.

La OMS se gobierna por una Asamblea General con representantes de todos los Estados Miembros, en total 196 Estados. La OMS dispones de un Consejo Ejecutivo integrado por 34 miembros cualificados profesionalmente en el ámbito de la salud, por un plazo de tres años.

La Unión Europea dispone del Centro europeo para la prevención y el control de las enfermedades (ECDC)[256]. Es una agencia de la Unión Europea creada en el año 2005 y cuya sede se encuentra en Estocolmo, Suecia. La Comisión Europea en julio de 2003 presentó un proyecto de ley para la creación del ECDC, fue aprobado mediante el Reglamento (CE) No 851/2004 del Parlamento Europeo y del Consejo el 21 de abril de 2004. El ECDC empieza a funcionar el 2005.

Las principales funciones del ECDC son las de analizar e interpretar los datos de los países de la UE sobre 52 enfermedades transmisibles, a través del Sistema Europeo de Vigilancia (TESSy), proporciona asesoramiento científico a los gobiernos e instituciones de la UE, garantiza la detección precoz y el análisis de las amenazas emergentes para la UE, coordina el Programa Europeo de Formación en Epidemiología de Intervención (EPIETEN)[257] y el Programa Europeo de Formación en Microbiología para la Salud Pública (EUPHEMEN) y ayuda a los gobiernos de la UE a prepararse contra los brotes de enfermedades[258].

5.6.3. La salud pública en el ordenamiento jurídico español

El ordenamiento jurídico español, en su ámbito estatal, hace referencia a la salud pública básicamente en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud y Ley 33/2011, de 4 de octubre, General de Salud Pública.

[256] ECDC. Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC). Comisión Europea. Web oficial de la Unión Europea. Disponible en https://europa.eu/european-union/ about-eu/agencies/ecdc_es (31/01/2021).

[257] EPIETEN. "Programa Europeo de Formación en Epidemiología de Intervención". Disponible es https://www.eurosurveillance.org/content/10.2807/esm.01.04.00171-es (28/02/2021).

[258] ECDC. Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC). Comisión Europea. Web oficial de la Unión Europea. Disponible en https://europa.eu/european-union/ about-eu/agencies/ecdc_es (31/01/2021).

La Ley 14/1986, de 25 de abril, General de Sanidad no dedica ningún Título, Capítulo o artículo específicamente a la salud pública, aunque, el capítulo V trata sobre la intervención pública en relación con la salud individual y colectiva. Esta Ley en su artículo 40 del capítulo I, sobre competencias del Estado dentro del Título II de las competencias de las Administraciones Públicas, en su punto 15 asigna en salud pública al Estado la competencia de elaboración de informes generales.

En cuanto al ámbito autonómico, la salud pública esta transferida a las Comunidades Autónomas lo cual ha dado pie a que en alguna de ellas se hayan aprobado leyes de salud pública, tale es el caso de la Ley 18/2009, de 22 de octubre, de salud pública de Cataluña; la Ley 10/2010, de 27 de septiembre, de salud pública y seguridad alimentaria de Castilla y León; la Ley 16/2010, de 28 de diciembre, de salud pública de las Islas Baleares; la Ley 7/2011, de 23 de marzo, de salud pública de Extremadura; la de Ley 16/2011, de 23 de diciembre, de Salud Pública de Andalucía; y la Ley 5/2014, de 26 de junio, de Salud Pública de Aragón.

La Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, ha sufrido una modificación en su artículo 4 a raíz del Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, previo a la aprobación del Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. Esta modificación es relativa al abastecimiento y distribución de determinados medicamentos y productos sanitarios.

El ordenamiento jurídico español define la existencia de una Red de Vigilancia de salud pública. Tal como menciona el preámbulo de la Ley 33/2011, se articula la Red de Vigilancia en salud pública que se ocupa de coordinar el sistema de vigilancia de factores condicionantes, el de problemas de salud y los sistemas de alerta precoz y respuesta rápida.

La Ley 33/2011 en su capítulo I (la vigilancia en salud pública) dentro de su Título II (Actuaciones en salud pública), dedica el artículo 12 a la vigilancia en salud pública diciendo, a tenor literal: “La vigilancia en salud pública es el conjunto de actividades destinadas a recoger, analizar, interpretar y difundir información relacionada con el estado de la salud de la población y los factores que la condicionan, con el objeto de fundamentar las actuaciones de salud pública”

A su vez, el artículo 13, sobre la articulación de la vigilancia en salud pública, crea una articulación diluida y poco eficaz, así lo expresa la Ley: “1. Corresponde a la Administración General del Estado, a las comunidades autónomas, a las ciudades de Ceuta y Melilla y a la Administración local, en el ámbito de sus competencias, la organización y gestión de la vigilancia en salud pública.”

En cuanto a las competencias del Ministerio de Sanidad en relación a la vigilancia en salud pública, el artículo 14 de la Ley 33/2011, le asigna la gestión de alertas de carácter supraautonómico y las que procedan de la Unión Europea, la Organización Mundial de

la Salud y demás organismos internacionales y, especialmente, de aquellas alertas contempladas en el Reglamento Sanitario Internacional[259].

También es competencia del Ministerio de Sanidad las alertas del artículo 65 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. Este artículo 65 establece lo que entiende por declaración de actuaciones coordinadas en salud pública. A su vez, determina que corresponderá al Ministerio de Sanidad y Consumo dicha declaración, aunque para ello deberá haber acuerdo del Consejo Interterritorial del Sistema Nacional de Salud. Sin embargo, todo ello con audiencia de las comunidades directamente afectadas. Sin embargo, el Ministerio de Sanidad podrá declarar la situación de "actuaciones coordinadas en salud pública" en situaciones de urgente necesidad tomando las medidas que sean estrictamente necesarias, informando de manera inmediata de las medidas adoptadas.

Las actuaciones coordinadas implican la utilización común de instrumentos técnicos, la configuración de una Red de Laboratorios de Salud Pública, la definición de estándares mínimos en el análisis e intervención sobre problemas de salud o la coordinación de sistemas de información epidemiológica y de programas de promoción, protección de la salud, prevención y control de las enfermedades más prevalentes.

En este orden de cosas, en base al artículo 14 de la Ley 33/2011, también son competencias del Ministerio de Sanidad en vigilancia de salud pública, la coordinación y evaluación de la Red de Vigilancia en salud pública y velar para que los criterios utilizados sean homogéneos y homologados.

A todo lo cual añade tanto el diseño como la ejecución de una encuesta periódica de salud pública en coordinación con las comunidades autónomas y ciudades de Ceuta y Melilla.

En este escenario el Ministerio de Sanidad coordinará y gestionará los intercambios de la información y los mensajes dirigidos a la población en el caso de que las Autoridades sanitarias emitieran comunicados o recomendaciones en contextos de alerta o crisis sanitarias o que afecten a riesgos inciertos que pudiesen afectar a más de una comunidad autónoma.

España tiene legislación especial en salud pública, la Ley 33/2011, de 4 de octubre, General de Salud Pública. Esta norma tan solo hace una referencia a las epidemias en su Disposición adicional cuarta. El término pandemia aparece en el capítulo artículo 33 (La actuación sanitaria en el ámbito de la salud laboral).

La Ley 33/2011 encomienda a los poderes públicos la función de la vigilancia en salud pública en el Capítulo I, mediante el artículo 12 (De la vigilancia en salud pública), el artículo 13 (Articulación de la vigilancia en salud pública) y el artículo 14 (De las

[259] OMS (2005) "Reglamento Sanitario Internacional (2005)". Tercera edición. Disponible en https://www.who.int/ihr/publications/9789241580496/es/ (28/02/2021).

competencias en Vigilancia en salud pública del Ministerio de Sanidad, Política Social e Igualdad).

El artículo 14 de la Ley 33/2011 encomienda la Ministerio de Sanidad la gestión de alertas de carácter supraautonómico o que puedan trascender del territorio de una comunidad autónoma y de alertas que procedan de la Unión Europea, la Organización Mundial de la Salud y demás organismos internacionales y, especialmente, de aquellas alertas contempladas en el Reglamento Sanitario Internacional, en su caso, en coordinación con las comunidades autónomas y las ciudades de Ceuta y Melilla. Las Actuaciones coordinadas en salud pública y en seguridad alimentaria del artículo 65 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, así como la coordinación y evaluación de la Red de Vigilancia en salud pública.

A modo de resumen, se observa que no existe un dispositivo claro y eficaz en materia de lucha contra las epidemias o pandemias en el ordenamiento jurídico español.

Nota crítica: con independencia de la respuesta del sistema sanitario a la demanda asistencial creada por la pandemia, se ha puesto de manifiesto que no se dispone a fecha de hoy (31/03/2021) todavía de la Red de Vigilancia de Salud Pública del artículo 13 de la Ley 33/2011, de 4 de octubre, General de Salud Pública y se sigue funcionando con la Red nacional de vigilancia epidemiológica creada en 1995.

5.6.4. El tratamiento de datos en una alarma en salud pública

5.6.4.1. Aspectos generales del tratamiento de datos personales en la gestión de una alarma sanitaria

En una epidemia los casos afectados se tratan a nivel clínico con los mismos datos que en cualquier otro supuesto. Los estudios y el seguimiento de una epidemia o de una pandemia son estudios de carácter poblacional. Los datos que se utilizan en la epidemiología, una de las ciencias que sustenta la disciplina de la salud pública, suelen ser datos personales, pero no identificables, es decir, si bien son datos relacionados con la salud de las personas, no son datos identificables. En estas circunstancias no se deben aplicar las normas de protección de datos vigentes.

El hecho de que los estudios epidemiológicos son estudios poblacionales y no requieran en un principio la identificación del dato nominal de la persona, no significa que en las actuaciones frente a determinadas alarmas sanitarias provocadas por epidemias no pueda hacer falta recurrir a la identificación de casos individualizados para proceder a su aislamiento y/o tratamiento.

Ejemplos de estos datos son el número de contagiados/día en una epidemia, en todo caso, estratificados por edad o por sexo. Estos datos que se utilizan en salud pública son remitidos de los centros sanitarios, anonimizados o seudonimizados a los centros de análisis y estudios epidemiológicos. Los datos también pueden ser remitidos por los servicios sanitarios centrales de los gobiernos en cuyo caso deben ir anonimizados o seudonimizados.

Sin embargo, las cláusulas que excluyen la regla o "cláusulas comodín" tanto del Reglamento (UE) 2016/679 como de la Ley Orgánica 3/2018, crean excepciones y bases jurídicas para la legitimación de una persona para el tratamiento de datos.

En el caso de que el tratamiento de datos fuera solo de carácter personal no de salud, en una situación de alarma de salud pública, podría aplicarse el artículo 6.1 en sus apartados d), e) o e). Así el apartado el c) menciona el hecho de que el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, el apartado d) hace referencia a que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física, o bien el apartado e) cuando mencionad que el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En el caso de que tenga que hacerse uso de datos personales relativos a la salud se debería acudir al artículo 9, lo cual se describe en el capítulo 5.5 del Título III.

El caso del tratamiento de datos personales no relativos a la salud de la persona pero que estaban protegidos por el RGPD y por la Ley Orgánica 3/2018, es el que se ha producido en la pandemia del COVID-19, en España.

La Ley Orgánica 4/1981, de 1 de junio de Estados de Alarma, Excepción y Sitio, en su artículo 6.1 establece que el estado de alarma se declara por el Consejo de Ministros mediante Real Decreto que no podrá exceder de los 15 días, prorrogable solo con autorización del Congreso de los Diputados. A su vez, determina que el Gobierno deberá presentar dicho Decreto al Congreso de los Diputados, artículo 8 de La Ley Orgánica. 4/1981, de 1 de junio de Estados de Alarma, Excepción y Sitio.

En este orden de cosas, el Gobierno aprobó el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 en marzo de 2020[260]. Posteriormente se declara el segundo Estado de Alarma[261] y posteriormente un tercer Estado de Alarma[262].

En base al Real Decreto 463/2020, el Ministerio de Sanidad emitió la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

Esta orden en su punto Segundo sobre DataCOVID-19: estudio de la movilidad aplicada a la crisis sanitaria, determina que:

> "Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, siguiendo el modelo emprendido por el Instituto Nacional de Estadística en su estudio de movilidad y a través

[260] *Vid. Infra p 384,* capítulo 3.5.3., del Título III.
[261] *Vid. Infra p 386,* capítulo 3.5.3., del Título III.
[262] *Vid. Infra p 388,* capítulo 3.5.3., del Título III.

> del cruce de datos de los operadores móviles, de manera agregada y anonimizada, el análisis de la movilidad de las personas en los días previos y durante el confinamiento.
>
> En la ejecución de este estudio, se velará por el cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos."

Aunque esta Orden SND/297/2020 no lo menciona, el artículo 6 del Reglamento (UE) 2016/679 y el artículo 8 de la Ley Orgánica 3/2018, son los que contienen las bases jurídicas para la legitimación de una persona frente a la excepción a estas normas. Sin embargo, es muy difícil de defender que el rango de esta norma sea suficiente para los fines a los cuales está destinada, es decir, regular derechos fundamentales, como es la protección de datos de carácter personal, sobre el que la Constitución Española, artículo 53 CE, establece una reserva de ley.

En los casos de materias reservadas a la Ley, como es este caso, cabe la colaboración reglamentaria, pero siempre que la ley haya establecido previamente los aspectos nucleares o esenciales de la regulación y siempre que esa regulación reglamentaria sea *"claramente dependiente y subordinada a la ley"* tal y como viene reiterando de forma asentada y univoca desde la aprobación de la Constitución Española por el Tribunal Constitucional[263] .

5.6.4.2. Las excepciones para permitir la licitud en el RGPD, las cláusulas comodín, a raíz de la alarma. Datos personales con carácter general

Las excepciones que devenguen de situaciones excepcionales como son las alertas en salud pública, en base al Considerando 45 del Reglamento (UE) 2016/679 deberán constar en el Derecho de la Unión o de los Estados miembros. Es decir, la excepción por sí sola no legitima si no hay una norma suficiente que ampare las acciones que se pretenden legitimar.

El artículo 6, establece la prohibición con carácter general para luego introducir puntos o cláusulas que excluyen de dicha prohibición en determinadas situaciones o supuestos, desde un punto de vista funcional cabe entender que estas excepciones actúan como cláusulas comodín.

Las situaciones de excepción que aparecen en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018 se comportan como supuestos de activación, la crisis en salud pública, en consecuencia, se deben incluir las alertas sanitarias producidas por una epidemia o pandemia.

En este sentido el Considerando 46 del Reglamento (UE) 2016/679 se refiere de forma explícita a las epidemias:

> "El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En

[263] STC 83/1984 (El Pleno) en FJ 3 y FJ5, STC 111/2014 (El Pleno) en FJ 4 y 139/2016 (El Pleno) en FJ 1, FJ 6 y FJ 7.

> 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."

El Considerando 45 del Reglamento (UE) 2016/679 entiende que cuando exista una obligación legal relativa al responsable del tratamiento o cuando exista una actuación en interés público o cuando la acción este ejercida por la autoridad pública, el tratamiento de los datos personales de categorías especiales debe tener una base en el Derecho de la Unión o de los Estados miembros. Es decir, la exclusión de la prohibición es posible si hay normas de aplicación, de rango suficiente, que regulen lo excepcionado.

Sin embargo, a pesar de estos Considerandos del RGPD la Agencia Española de Protección de Datos, en su informe de abril de 2020, entiende que la base jurídica del tratamiento de datos personales durante la gestión de la pandemia por CIVD-19 se establece a través de artículo 6.1e) y artículo 6.1.d) del Reglamento (UE) 2016/679 Reglamento (UE) 2016/679, sin especificar las normas del ordenamiento jurídico español que serían de aplicación o bien la necesidad de legitimar mediante leyes estás excepciones. El primero de ellos hace referencia a "la misión realizada en interés público" y el segundo "a los intereses vitales del interesado u otras personas físicas".

5.6.4.3. Las garantías del RDGP en el tratamiento de datos en la alarma sanitaria

La gestión de la pandemia en cualquier circunstancia debe estar amparada por una norma que fije todas estas garantías que aparecen en el RGPD y en la Ley Orgánica 8/2018, tales como: la licitud, la lealtad y la transparencia, en relación al interesado, artículo 5.1.a RGPD, la limitación de la finalidad, artículo 5.1.b RGPD, la minimización de datos, artículo 5.1.c RGPD, la exactitud de los datos, y actualización, artículo 5 del RGPD y artículo 4 de LO 3/2018, la confidencialidad artículo 5 del RGPD y artículo 6 de LO 3/2018, la Licitud de tratamiento, artículo 6 RGPD, el consentimiento, artículo 7 del RGPD y art. 6 de LO 3/2018, los principios que rigen las categorías especiales de datos, artículo 9 RGPD; y otros principios como: el del periodos de conservación limitados, calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento y las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes, artículo 47 del RGPD.

En este orden de cosas seguiremos con una serie de consideraciones en relación al consentimiento, a los principios de licitud, lealtad y transparencia y a los principios de limitación de la finalidad y minimización de datos.

Consideraciones:

Consideración. A. El consentimiento

El consentimiento debe ser dado de forma libre, totalmente libre, lo cual no se cumple cuando el consentimiento se da bajo la amenaza de denegación de un derecho, por ejemplo, derecho de acceso a una determinada ubicación[264].

Por lo tanto, los fundamentos que legitiman los tratamientos de datos personales y de salud por apps o páginas web de autoevaluación, aplicaciones de rastreo o procedimientos de toma de temperatura son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas. Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia.

Cuando las autoridades públicas prestan un servicio basado en un mandato atribuido por la legislación y acorde con los requisitos legales vigentes, la base jurídica más adecuada para el tratamiento de datos es la necesidad de cumplir una misión de interés público, es decir, el artículo 6.1.e) RGPD.

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

Consideración. B. Los principios de "licitud, lealtad y transparencia"

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

El principio de "licitud" significa que el tratamiento de datos personales sólo será lícito si puede justificarse en alguna de las bases jurídicas previstas en el artículo 6.1, en datos personales con carácter general, y en el artículo 9, ambos del RGPD, para el caso de datos de la salud.[265]

Los principios de "lealtad y transparencia" se concretan de dos formas, el de lealtad, con el cumplimiento formal y material de los derechos de los afectados por el tratamiento[266], el de transparencia, a través del conocimiento necesariamente informado por parte del interesado de la finalidad o finalidades concretas del tratamiento al que se van a someter sus datos[267]. El principio de lealtad se verá infringido en el caso de que los datos personales hayan sido obtenidos de una manera engañosa

[264] "De acuerdo con el Considerando 32 RGPD y las directrices específicas marcadas por el GT29, el consentimiento deberá ser otorgado libremente, de forma específica, informada e inequívoca, mediante una acción terminante afirmativa y sin que el silencio o la inacción del interesado signifiquen aceptación del tratamiento". GT29, Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, WP259 y rev. 01, revisadas por última vez y adoptadas el 10 de abril de 2018. Disponible en https://www.euskadi.eus/ contenidos/ informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf.

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

[266] LÓPEZ ÁLVAREZ, L.F. (2017) "Protección de datos personales: adaptaciones necesarias al nuevo Reglamento Europeo". Madrid- Ed. Lefebvre. p 31.

[267] GÓMARA HERNÁNDEZ, J.L. (2018) "Protección de Datos: el RGPD en las Entidades Locales", Barcelona, Ediciones Lefebvre. p 85.

para el interesado. La proyección del principio de transparencia, es el presupuesto necesario para el ejercicio de todos los derechos de los titulares de datos personales reconocidos por el RGPD.

Consideración. C. Los principios de «limitación de la finalidad» y "minimización de datos"

Consideración. C). 1. Limitación de la finalidad

El tratamiento de datos personales, en cualquier caso, se fundamenta en una adecuada base jurídica, lo que conlleva el reconocimiento de los principios de limitación de la finalidad, artículo 5.1.b RGPD, y minimización de datos, artículo 5.1.c RGPD.

El artículo 5.1.b) RGPD dispone que los datos personales serán:

> "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; […] el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)".

Respecto del requerimiento relativo al "uso o tratamiento compatible", significa que los datos personales no pueden ser tratados de una manera incompatible con la finalidad para la cual fueron recabados inicialmente en un tratamiento ulterior[268].

Consideración. C). 2. Minimización de datos

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

I. delimitar cuál es la finalidad para la que se recaba
II. determinar si cada actividad de tratamiento es realmente necesaria para conseguir la finalidad propuesta

El principio de minimización se encuentra íntimamente conectado con los principios de limitación de la finalidad, necesidad y proporcionalidad. En este sentido, la minimización introduce, por un lado, un elemento de razonabilidad, en el sentido de que los datos que se traten deberán ser los oportunos y apropiados para la finalidad que justifique el

[268] De acuerdo con el GT29, por «tratamiento ulterior» debe entenderse cualquier tratamiento subsiguiente a la recogida de los datos personales, ya sea de acuerdo con las finalidades inicialmente especificadas o para finalidades adicionales. Pues bien, cualquier tratamiento ulterior, debe ser compatible con la finalidad inicial. A la hora de determinar la «compatibilidad» entre un tratamiento ulterior y la finalidad inicial, el GT29 ha delimitado los siguientes factores clave. Vid. GT29, Opinión 03/2013,on purpose limitation, 2 de abril de 2013, apartado III.2.2.

tratamiento; y por otro, un elemento de proporcionalidad, de manera que el exceso de los datos tratados resultaría ilícito. [269]

Además, ha de señalarse que tanto el CEPD[270] como la AEPD entienden que las aplicaciones tecnológicas que se pueden poner en marcha para el seguimiento del COVID no pueden ni deben sustituir al conocido habitualmente por rastreo manual de contactos el cual es realizado por personal sanitario cualificado (en particular, de las entrevistas con personas infectadas) que puede determinar si los contactos estrechos pueden o no dar lugar a una transmisión del virus. Es decir, debe formar parte de un programa de salud pública normalizado.

En la medida de que el tratamiento de datos personales se haga necesario para la gestión de la pandemia de COVID-19, la protección de datos será imprescindible para generar confianza y sentar las condiciones para la aceptación social de cualquier solución y, así, garantizar la eficacia de las medidas adoptadas. Del mismo modo, debe subrayarse que la normativa europea en materia de protección de datos permite el uso responsable de datos personales para fines de gestión sanitaria, al tiempo que garantiza que en ese proceso no se erosionen los derechos y libertades individuales[271].

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

5.6.5. Orientaciones de la Comisión Europea sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia en lo referente a la protección de datos.

El Boletín Oficial de la Unión Europa publica el día 17 de abril de 2020 el documento "La Comisión Europea Comunicación 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 2020/C 124 I/01".

Estas orientaciones solo se refieren a aplicaciones de carácter voluntario para el apoyo a la lucha contra la pandemia de COVID-19, aplicaciones descargadas, instaladas y utilizadas de forma voluntaria por los ciudadanos, que tengan una o varias de las funcionalidades siguientes:

a. facilitar información exacta a las personas sobre la pandemia de COVID-19

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

[270] Comité Europeo de Protección de Datos.

[271]Directrices 04/2020 del Comité Europeo de Protección de Datos, de 21 de abril, sobre el uso de datos de localización de herramientas de rastreo de contactos en el contexto de pandemia de COVID-19. Disponible en https://edpb.europa.eu/sites/edpb/files/files/file1/ edpb_guidelines_20200420_ contact_ tracing_covid_with_annex_es.pdf. (28/02/2021).

b. ofrecer cuestionarios de autoevaluación y orientación a los ciudadanos (funcionalidad de comprobación de síntomas)
c. alertar a las personas que hayan estado cerca de una persona infectada durante un tiempo determinado, a fin de proporcionar información, por ejemplo, sobre la conveniencia de someterse a una auto-cuarentena y de hacerse las pruebas (funcionalidad de rastreo de contactos y de alerta)
d. proporcionar un foro de comunicación entre médicos y pacientes en autoaislamiento o en el que se brinden consejos adicionales en materia de diagnóstico y tratamiento (mayor recurso a la telemedicina).

El documento con nueve páginas contiene un primer punto sobre el contexto, al cual le sigue un segundo apartado "Contribución de las aplicaciones a la lucha contra el COVID-19". El apartado tercero de la comunicación versa sobre "Elementos para un uso fiable y responsable de las aplicaciones".

El tercer apartado describe un conjunto de diez recomendaciones. Estas recomendaciones contemplan tres tipos de funcionalidades: de información, de comprobación de síntomas y de telemedicina y de rastreo de contactos y de alerta.

Estas diez recomendaciones son:

1.ª Autoridades sanitarias nacionales como responsables del tratamiento de datos.

Determinar el responsable del tratamiento: quién decide los medios y los fines del tratamiento de datos. La Comisión considera las autoridades sanitarias nacionales deben ser las responsables del tratamiento.

2.ª Garantizar que la persona siga teniendo el control:

- La instalación de la aplicación: voluntaria.
- No agrupar distintas funcionalidades en una sola aplicación.
- Datos de proximidad: deben almacenarse en el dispositivo de la persona.
- Acceso total a la información necesaria en relación con el tratamiento.
- Derechos de acceso, rectificación y supresión.
- Desactivación automática al finalizar la pandemia.

3.ª Base jurídica para el tratamiento:

a) Instalación de las aplicaciones y almacenamiento de información en el dispositivo del usuario: en base al consentimiento y a la estricta necesidad.
b) Base jurídica para el tratamiento por parte de las autoridades sanitarias nacionales, Derecho de la Unión o de un Estado miembro,: todo instrumento legislativo nacional ha de prever medidas específicas y adecuadas para salvaguardar los derechos y las libertades de los titulares de los datos.

4.ª Minimización de datos: viene exigida por el RGPD y contemplada en:

a) Datos personales: artículo 4, apartado 1, del RGPD.
b) Datos relativos a la salud: artículo 9 del RGPD.

c) Datos de localización: artículo 5, apartado 1, y artículos 6 y 9 de la Directiva sobre la privacidad y las comunicaciones electrónicas

d) Información almacenada en el equipo terminal del usuario y a la que se acceda desde dicho equipo: artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

5.ª Limitar el acceso a los datos y su divulgación

6.ª Tratamiento de los datos con fines precisos. Datos de personas infectadas y datos de las personas que han estado en contacto, epidemiológico, con la persona infectada

7.ª Establecimiento de límites estrictos al almacenamiento de datos

8.ª Garantizar la seguridad de los datos

9.ª Garantizar la exactitud de los datos

10.ª Involucrar a las autoridades de protección de datos

TÍTULO II. INSTITUCIONES DE CONTROL, REGULACIÓN, TRATAMIENTO, COOPERACIÓN Y AUTORREGULACIÓN EN EL REGLAMENTO DE PROTECCIÓN DE DATOS

Señala RODRÍGUEZ DE SANTIAGO, que la organización es "la estructura institucional que se encarga de ofrecer y realizar las prestaciones a favor de sus destinatarios (…) -para crear el marco organizativo completo en el que actúan los sujetos que intervienen en el desarrollo de las prestaciones"[272]. Y, en el caso del derecho a la protección de datos de carácter personal constituye un ejemplo singular de estructura institucional, compuesta por una diversidad de figuras organizativas:

- Las autoridades de control independientes: el Capítulo VI del Reglamento (UE) 2016/679 regula los parámetros, competencias, funciones y poderes de dichas autoridades de control. Para ello, ordena el artículo 51.1 que:

  > "cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante "Autoridad de control") supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión".

  Estas autoridades de control deberán ser constituidas por Ley, que deberá, en todo caso, abarcar el contenido que se señala en el artículo 54.1 del citado Reglamento[273]. Y, adicionalmente, las autoridades de control actuarán con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes, artículo 52.1 del Reglamento (UE) 2016/679. De forma particular, en nuestro país, el Título VII de la Ley Orgánica 3/2018 contiene la regulación propia para la Agencia Española de Protección de Datos, Capítulo I, y para las Autoridades Autonómicas de Protección de Datos, Capítulo II.

- El Supervisor Europeo de Protección de Datos: es la autoridad independiente de la Unión Europea en materia de protección de datos. Su regulación se encuentra contenida en el Capítulo VI del Reglamento (UE) 2018/1725 del Parlamento Europeo y

[272] RODRÍGUEZ DE SANTIAGO, J.M. (2007) "La Administración del Estado social". Madrid. Marcial Pons. p 140.

[273] Este precepto del Reglamento (UE) 2016/679 dispone que: "cada Estado miembro establecerá por ley todos los elementos indicados a continuación: a) el establecimiento de cada autoridad de control; b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control; c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control; d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado; e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse; f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo".

del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE. El artículo 52 del citado Reglamento define las dos funciones esenciales del Supervisor: (i) velar por que los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la protección de datos, sean respetados por las instituciones y organismos de la Unión; (ii) garantizar y supervisar la aplicación del Reglamento (UE) 2018/1725 y de cualquier otro acto de la Unión relacionado con la protección de los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales por parte de una institución u organismo de la Unión, y asesorar a las instituciones y organismos de la Unión, así como a los interesados, en las cuestiones relacionadas con el tratamiento de datos personales. Los artículos 57 y 58 del Reglamento (UE) 2018/1725 detallan sus funciones y competencias, respectivamente. En todo caso, el ejercicio de tales funciones y competencias deberá realizarse bajo un principio de independencia, conforme al artículo 59.

- El Comité Europeo de Protección de Datos: se configura como un organismo europeo independiente que tiene por objeto contribuir a dotar de uniformidad la aplicación de la normativa de protección de datos a nivel europeo y a facilitar la cooperación entre las autoridades de protección de datos de los distintos países de la Unión Europea. Conforme al artículo 68.1 del Reglamento (UE) 2016/679, dicho Comité es un organismo de la Unión Europea que goza de personalidad jurídica. Sus funciones principales son: velar por una aplicación coherente del Reglamento (UE) 2016/679, incluso mediante la emisión de resoluciones vinculantes respecto a las autoridades de control de cada Estado miembro; asesorar a la Comisión Europea en materia de protección de datos; y emitir dictámenes, directrices, recomendaciones y buenas prácticas en la materia[274]. Para el desempeño de esas funciones, el Comité actuará con total independencia, conforme al artículo 69 del Reglamento (UE) 2016/679.

- El delegado de protección de datos: los artículos 37 a 39 del Reglamento (UE) 2016/679 dotaron de carta de naturaleza a la figura del delegado de protección de datos, figura creada por primera vez en la legislación alemana en 1977[275]. El delegado de protección de datos se erige como una figura de supervisión, información y asesoramiento interno al responsable o al encargado del tratamiento. No es, pues, una institución pública, sino una figura que se incardina dentro de la propia estructura del responsable o encargado del tratamiento.

A continuación, nos detenemos en el estudio pormenorizado de estas figuras y de sus herramientas básicas de actuación.

[274] El artículo 70 del Reglamento (UE) 2016/679 regula con detalle las funciones del Comité Europeo de Protección de Datos.

[275] El Bundesbeauftragten für den Datenschutz fue creado por la Ley Federal de Protección de Datos de 27 de enero de 1977 (Bundesdatenschutzgesetz).

Capítulo 1. Los Órganos de Control

1.1. El Órgano de Control de la UE

1.1.1. Cuestiones preliminares

La Comisión Europea tiene su fundamento jurídico en el artículo 17 del Tratado de la Unión Europea (TUE) y en los artículos 234, 244 a 250, 290 y 291 del Tratado de Funcionamiento de la Unión Europea (TFUE) y el Tratado por el que se constituye un Consejo único y una Comisión única de las Comunidades Europeas (Tratado de Fusión)

En el año 2009 el Consejo Europeo decidió que el número de miembros de la Comisión Europea fuera el mismo que el número de países miembros. La Comisión Europea dispone de un presidente que es propuesto por el Consejo Europeo, teniendo en cuenta el resultado de las elecciones al Parlamento Europeo, propondrá la Parlamento Europeo un candidato a presidente de la Comisión, por mayoría cualificada. El Parlamento elige y nombre al candidato como presidente del Comisión Europea por mayoría de los miembros que lo componen, artículo 17, apartado 7, de TUE.

El Consejo de la Unión Europea, por mayoría cualificada, y de acuerdo con el presidente de la Comisión Europea aprueba la lista de los demás cargos públicos que componen la Comisión Europea, de conformidad con las propuestas presentadas por cada estado miembro.

El presidente y demás miembros del Comité Europeo, incluido el alto representante de la Unión Europea para asuntos exteriores y política de seguridad, se someten colegiadamente al voto de aprobación del Parlamento y, a continuación, son nombrados por el Consejo Europea, por mayoría cualificada.

La Comisión Europea es la Institución de la Unión Europea que tiene la iniciativa legislativa e importantes poderes ejecutivos. Es el principal órgano ejecutivo de la Unión Europea y está formada por un colegio de comisarios compuesto por un representante por cada Estado miembro.

La Comisión Europea supervisa la aplicación del Derecho de la Unión Europea y el respeto a los Tratados de la Unión por parte de los Estados miembros, además preside los comités para la aplicación del Derecho de la Unión. En relación a los Reglamentos, la Comisión Europea supervisa su cumplimento.

El Reglamento (UE) 2016/679 en su artículo 68 crea el Comité Europeo de Protección de Datos, que en el RGPD también aparece con la denominación de Comité, como organismo de la Unión, que gozará de personalidad jurídica. El comité está compuesto por un presidente y por el director de una autoridad de control de cada Estado miembro.

La Comisión en relación con el Comité, tendrá derecho a participar en sus actividades y reuniones, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité Europeo de Protección de Datos, artículo 68 del Reglamento (UE) 2016/679. Además, la Comisión podrá solicitar que el Comité cumpla sus funciones a efectos de la aplicación del Reglamento

(UE) 2016/679, artículo 70.1 del Reglamento (UE) 2016/679, así como su asesoramiento, señalando un plazo teniendo en cuenta la urgencia del asunto, artículo 70.2 del Reglamento (UE) 2016/679. La Comisión, conocerá el Informe anual del Comité, artículo 71 del Reglamento (UE) 2016/679.

La Comisión tiene una serie de funciones en el Reglamento (UE) 2016/679 que incluyen fijar cláusulas contractuales tipo[276], artículo 28.7 del Reglamento (UE) 2016/679 así como promover la elaboración de códigos de conducta, junto con los Estados miembros y las autoridades de control, artículo 40.1 del Reglamento (UE) 2016/679. Le corresponde mediante actos de ejecución, decidir sobre la validez de los Códigos de Conducta, artículo 40.9 del Reglamento (UE) 2016/679 y publicar su contenido una vez aprobados, artículo 40.10 del Reglamento (UE) 2016/679.

La Comisión junto con los Estados miembros, las autoridades de control y el Comité promoverá la creación de mecanismos de certificación, aportando normas técnicas, y su reconocimiento en materia de protección de datos y de sellos y marcas de protección de datos, artículos 42.1 y 43.9 del Reglamento (UE) 2016/679, mediante actos de ejecución, artículo 43.9 del Reglamento (UE) 2016/679. Pudiendo adoptar actos delegados para especificar las condiciones para los mecanismos de certificación en materia de protección de datos, artículo 43.8 del Reglamento (UE) 2016/679.

La Comisión en materia de cooperación internacional junto con las autoridades de control, tomarán medidas apropiadas para facilitar la aplicación eficaz de la legislación relativa a la protección de datos personales; para la asistencia mutua; para asociar a partes interesadas y promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, artículo 50 del Reglamento (UE) 2016/679.

La cooperación con las autoridades de control para el fin del RGPD, artículo 51.1 del Reglamento (UE) 2016/679, es otra de sus funciones, disponiendo anualmente del informe de actividades emitido por cada una de ellas, artículo 59 del Reglamento (UE) 2016/679.

Los Estados miembros notificaran a la Comisión las disposiciones legales que estos adopten conforme al Reglamento (UE) 2016/679, artículo 51.2 del Reglamento (UE) 2016/679.

Cuando un asunto de aplicación general, o que surta efecto en más de un Estado miembro, tenga relación con el RGPD y en base al principio de la asistencia mutua podrá solicitar su examen por el Comité a efectos de dictamen, en particular cuando una

[276] COMISIÓN EUROPEA. Decisión de la comisión, 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri= CELEX: 32010D0087 &from=ES (28/02/2021).

autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua, artículo 64 del Reglamento (UE) 2016/679.

1.1.2.Los actos de ejecución

El Parlamento y el Consejo pueden apoderar a la Comisión para adoptar diversos actos, unos serán actos delegados y los otros actos serán actos de ejecución, con el objeto garantizar la aplicación de una ley de la UE.

La legislación de la UE tiene un solo objeto, su cumplimiento por los Estados miembros y su aplicación en toda la Unión Europea. En este orden de cosas, son los Estados miembros los que deben ejecutar la legislación de la UE, aunque la Comisión puede adoptar "actos de ejecución" para aplicar condiciones uniformes de aplicación de la legislación de la UE.

Los actos de ejecución son distintos de los actos delegados, que son esas disposiciones de la Comisión en virtud de una delegación otorgada a través de una ley de la UE.

En base al Reglamento (UE) 2016/679 la Comisión Europea podrá adoptar actos de ejecución, con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2, en los siguientes supuestos:

1. sobre la validez del Código de Conducta o la modificación o ampliación aprobados y presentados, artículo 40.9 del Reglamento (UE) 2016/679.
2. adoptar normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, artículo 43.9 del Reglamento (UE) 2016/679.
3. adoptar mecanismos para promover y reconocer los mecanismos de certificación, sellos y marcas, artículo 43.9 del Reglamento (UE) 2016/679.
4. podrá derogar, modificar o suspender, en la medida necesaria y sin efecto retroactivo, la decisión de adecuación que evalúa la adecuación del nivel de protección, artículo 45.5 del Reglamento (UE) 2016/679.
5. podrá especificar el formato y los procedimientos de asistencia mutua, así como las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité, artículo 61.9 del Reglamento (UE) 2016/679.
6. podrá especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité, en especial el formato normalizado contemplado en el artículo 64, artículo 67.1 del Reglamento (UE) 2016/679.

1.1.3. La Comisión y las decisiones de adecuación

Una decisión de adecuación es en realidad un acto de ejecución, es decir, un acto jurídico realizado por la Comisión Europea y habilitado en este caso por el RGPD, Directiva 2016/680 y el artículo 288 del TFUE que permite declarar que un tercer Estado dispone de un nivel de protección adecuado a las exigencias de la UE. Mediante este acto jurídico la Comisión autoriza la transferencia internacional de datos con terceros a la Unión Europea, mediante la cual la Comisión acepta que ese país, región, u organización internacional tiene un nivel de protección adecuado de los datos de las personas, sin necesidad de autorización singular de alguna Autoridad de Supervisión[277].

En materia de decisiones de adecuación, podrá adoptar una "decisión de adecuación" cuando entienda que existen garantías de protección de datos personales adecuados de un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate, artículo 45 del Reglamento (UE) 2016/679.

La Comisión podrá decidir sobre la garantía de protección de datos que ofrece u tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate, artículo 45.1 del Reglamento (UE) 2016/679, a tales efectos, supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales, artículo 45.4 del Reglamento (UE) 2016/679.

Además de su capacidad para aprobar decisiones de adecuación también podrá derogarlas mediante un acto de ejecución cuando un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantice el nivel de protección adecuado exigido por el Reglamento (UE) 2016/679, artículo 45.5 del Reglamento (UE) 2016/679.

1.2. Comité Europeo de Protección de datos

1.2.1. Naturaleza y composición. Confidencialidad e independencia

El Comité Europeo de Protección de Datos (CEPD)[278] es el organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE[279].

El antecedente de esta figura se encuentra en el artículo 29 de la Directiva 95/46/CE del Parlamento y del Consejo de 24 de octubre de 1995, mediante la denominación de "Grupo de protección de las personas en lo que respecta al tratamiento de datos personales".

[277] GONZALO DOMENECH JJ. 2019) "Las decisiones de adecuación en el derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de aplicación por los Estados Miembros". Cuadernos de Derecho Transnacional. 11 (1), 350-371. p 355.

[278] ECDC. Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC). Comisión Europea. Web oficial de la Unión Europea. Disponible en https://europa.eu/european-union/ about-eu/agencies/ecdc_es (31/01/2021).

[279] COMISIÓN EUROPEA. Web oficial de la Unión Europea. "Comité Europea de Protección de Datos". Disponible en https://edpb.europa.eu/about-edpb/about-edpb_es (28/02/2021).

El Reglamento (UE) 2016/679 en su sección 3ª y concretamente en su artículo 68 crea el Comité Europeo de Protección de Datos, organismo con personalidad jurídica propia, compuesto por un presidente, artículo 73 del Reglamento (UE) 2016/679), una secretaria, artículo 73 del Reglamento (UE) 2016/679, y por el director de la Autoridad de control de cada Estado Miembro, por el Supervisor Europeo de Protección de Datos y un representante de la Comisión Europea.

Los principios rectores que regulan e inspiran al Comité Europeo de Protección de Datos son: la independencia e imparcialidad; la buena gobernanza, integridad y buena conducta administrativa; la responsabilidad colegial; la cooperación; la transparencia; la eficiencia y modernización; y la proactividad.

El Comité Europeo elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión, artículo 71 del Reglamento (UE) 2016/679. El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas indicadas en el artículo 70, apartado 1, letra l), así como de las decisiones vinculantes indicadas en el artículo 65.

Los debates del Comité serán confidenciales cuando el mismo lo considere necesario, tal como establezca su reglamento interno, artículo 76 del Reglamento (UE) 2016/679.

El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71 del Reglamento (UE) 2016/679. El Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias, sin perjuicio de las solicitudes de la Comisión Europea, artículo 69 del Reglamento (UE) 2016/679.

1.2.2. Funciones del Comité Europeo de Protección de Datos

Las funciones, artículo 70 del Reglamento (UE) 2016/679, del Comité Europeo de Protección de Datos (en adelante también, El Comité) abarcan la supervisión y garantía de la correcta aplicación del presente Reglamento en los casos contemplados en los artículos 64 y 65 del Reglamento (UE) 2016/679, asesorar a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del presente Reglamento y asesorar el formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes.

Por otra parte, el Comité emitirá directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública a que se refiere el artículo 17, apartado 2 Reglamento (UE) 2016/679.

Podrá examinar de oficio o a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, emitiendo

directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del Reglamento (UE) 2016/679.

Emitirá directrices, recomendaciones y buenas prácticas de conformidad con la letra e) del artículo 70.1 dentro del Reglamento (UE) 2016/6799, a fin de:

- Especificar los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22 del Reglamento (UE) 2016/679.
- Especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47.
- Especificar en mayor medida los criterios y requisitos de las transferencias de datos personales sobre la base del artículo 49, apartado 1.
- Establecer procedimientos comunes de información procedente de personas físicas sobre infracciones del presente Reglamento en virtud del artículo 54, apartado 2.
- Constatar las violaciones de la seguridad de los datos y determinar la dilación indebida, con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales.
- Con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 34, apartado 1.

El Comité formulará directrices para las autoridades de control, relativas a la aplicación de las medidas a que se refiere el artículo 58, apartados 1, 2 y 3, y la fijación de multas administrativas de conformidad con el artículo 83 del Reglamento (UE) 2016/679.

El Comité al igual que la Comisión alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad con los artículos 40 y 42 del Reglamento (UE) 2016/679.

Realizará la acreditación de los organismos de certificación y su revisión periódica en virtud del artículo 43 del Reglamento (UE) 2016/679, y llevará un registro público de los organismos acreditados en virtud del artículo 43, apartado 6, del Reglamento (UE) 2016/679 y de los responsables o los encargados del tratamiento acreditados establecidos en terceros países en virtud del artículo 42, apartado 7 del Reglamento (UE) 2016/679. Así también, especificará los requisitos contemplados en el artículo 43, apartado 3, con miras a la acreditación de los organismos de certificación en virtud del artículo 42 del Reglamento (UE) 2016/679 y facilitará a la Comisión y elaborará dictámenes:

a. sobre los requisitos de certificación contemplados en el artículo 43, apartado 8 del Reglamento (UE) 2016/679,
b. sobre los iconos a que se refiere el artículo 12, apartado 7 del Reglamento (UE) 2016/679,
c. sobre los proyectos de decisión de las autoridades de control en virtud del mecanismo de coherencia mencionado en el artículo 64, apartado 1, sobre los asuntos presentados en virtud del artículo 64, apartado 2, y sobre las decisiones vinculantes en virtud del artículo 65[280], incluidos los casos mencionados en el artículo 66 del Reglamento (UE) 2016/679,
d. sobre los códigos de conducta elaborados a escala de la Unión de conformidad con el artículo 40, apartado 9 del Reglamento (UE) 2016/679,
e. para evaluar la adecuación del nivel de protección en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado.

El Comité promoverá la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control, promoviendo programas de formación comunes y facilitará intercambios de personal entre las autoridades de control y, cuando proceda, con las autoridades de control de terceros países o con organizaciones internacionales y el intercambio de conocimientos y documentación sobre legislación y prácticas en materia de protección de datos con las autoridades de control encargadas de la protección de datos a escala mundial.

Finalmente, el Comité llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

1.2.2.1. La decisión de adecuación (La decisión de adecuación del Comité)

Una decisión de adecuación es equivalente a una Decisión de Ejecución y es competencia de la Comisión Europea, artículo 45 del Reglamento (UE) 2016/679 y será informado y evaluado por Comité Europeo de Protección de Datos, artículo 10.1.s) del Reglamento 2016/679. La decisión de adecuación es un dictamen o acto de ejecución conforme al cual decide que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección, especificando su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control competente.

La decisión de adecuación viene regulada en el artículo 45 del Reglamento (UE) 2016/679 y referida en el artículo 131.f., artículo 14.1.f, artículo 46.1 y 46.5, artículo 49.1 y 49.5, Considerando 104 y Considerando 112.

[280] STJUE de 16 de julio de 2020 (Gran sala) (asunto C-311/18) apartado 147, p 39.

Esta decisión tiene naturaleza de acto jurídico realizado por la Comisión Europea y habilitado en este caso por el RGPD, Directiva 2016/680 y el artículo 288 del TFUE que permite declarar a un tercer Estado, o a una Organización Internacional, con un nivel de protección adecuado sin necesidad de autorización singular de alguna Autoridad de Supervisión[281]. Lo cual tendrá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional.

La decisión de adecuación permitirá que un país miembro de la Unión Europea remita o trasmita datos o realice una transferencia de datos personales a un tercer país u organización internacional din necesidad de autorización específica.

La decisión de adecuación es la máxima garantía de adecuación de datos personales para un tercer país o para una Organización internacional, pero no es la única, tal como consta en el artículo 46 y artículo 49 del Reglamento (UE) 2016/679

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, artículo 32 del Reglamento (UE) 2016/679.

La decisión de adecuación se incardina dentro de los mecanismos de coherencia a través de las normas corporativas vinculantes y los dictámenes del Comité.

Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: el Estado de Derecho y el respeto de los derechos humanos y las libertades fundamentales. Tendrá en cuenta, la legislación pertinente y la aplicación de dicha legislación, tanto general como sectorial, incluida la relativa:

1. la seguridad pública
2. la defensa
3. la seguridad nacional
4. la legislación penal
5. el acceso de las autoridades públicas a los datos personales
6. las normas de protección de datos
7. las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional

La Comisión, al evaluar la adecuación del nivel de protección, analizará la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos.

[281] GONZALO DOMENECH JJ. (2019) “Las decisiones de adecuación …..”, op.cit; p 355.

Se deberá tener en cuenta, la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros y los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

A fecha de 31 de marzo de 2021, la Comisión ha emitido decisiones de adecuación para los siguientes países, por orden cronológico de la decisión de adecuación, del más antiguo al más reciente:

1. Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000
2. Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos
3. Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003
4. Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003
5. Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004
6. Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008
7. Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010
8. Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010
9. Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011
10. Uruguay. Decisión 2012/484/UE, de la Comisión de 21 de agosto de 2012.
11. Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012
12. Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.
13. Japón. Decisión de 23 de enero de 2019

En este orden de cosas, el Comité ha debido realizar un Dictamen en el proceso de salida del ICO (Autoridad de control inglesa) con motivo del Brexit y deberá proceder a la decisión de adecuación sobre el Reino Unido a partir del 31 de enero de 2020[282].

Finalmente, hay que apuntar que el TJUE ha invalidado una decisión de adecuación que hace referencia a los EEUU en su Sentencia C362/14 de 6 de octubre de 2015 por falta de protección de los datos personales en tercer país. Concretamente dice la sentencia en su última página, en "declara: 2) La Decisión 2000/520 es inválida"[283].

[282] GASCÓN MARCÉN, A. (2020) "La regulación del flujo de los datos personales entre la Unión Europea y el Reino Unido tras el Brexit". Cuadernos de Derecho Transnacional, 12 (1), 231-246. p 225.

[283] STJUE de 6 de octubre de 2015 (Gran sala) (asunto C-362/14), apartado el Tribunal de Justicia Declara, última p.

1.2.3.El Supervisor Europeo de Protección de Datos

El Supervisor Europeo de Protección de Datos es la Autoridad de control independiente que supervisará la aplicación de las disposiciones del Reglamento (UE) 45/2001 en todas las operaciones de tratamiento realizadas por las instituciones y organismos comunitarios y velará por los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la intimidad, sean respetados por las instituciones y los organismos comunitarios, por lo que respecta al tratamiento de los datos personales, artículo 41, Reglamento (CE) No 45/2001.

El Supervisor Europeo de Protección de Datos es nombrado de común acuerdo por el Parlamento Europeo y el Consejo, por un mandato de cinco años, sobre la base de una lista elaborada por la Comisión como resultado de una convocatoria pública de candidaturas. Se nombrará a un Supervisor Adjunto de conformidad con el mismo procedimiento y por un periodo de igual duración que asistirá al Supervisor en todas sus funciones y le sustituirá en caso de ausencia o impedimento.

El Supervisor Europeo de Protección de Datos es una figura que aparece en el artículo 68 del Reglamento (UE) 2016/679 que atiende a la creación del Comité Europeo de Protección de Datos.

El Supervisor Europeo de Protección de Datos en el ámbito del Reglamento (UE) 2016/679, es miembro del Comité Europeo de Protección de datos, artículo 68, apartado 3, del Reglamento (UE) 2016/679, ocupa la Secretaría del Comité Europeo de Protección de Datos, artículo 75, apartado 1, del Reglamento (UE) 2016/679, y además tendrá voto en las decisiones relativas a los principios y normas aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento, artículo 68, apartado 6, del Reglamento (UE) 2016/679.

La función principal del Supervisor Europeo de Protección de Datos es garantizar que, a la hora de tratar datos personales, las instituciones y organismos de la UE respeten el derecho a la intimidad de los ciudadanos, artículo 41, Reglamento (CE) No 45/2001. Son sus funciones y/o potestades:

A) Supervisa el tratamiento de los datos personales por parte de la administración de la UE, a fin de garantizar el cumplimiento de las normas de protección de la intimidad y las nuevas tecnologías que puedan tener una incidencia en la protección de datos.
B) Asesora a las instituciones y los organismos de la UE sobre todo lo relativo al tratamiento de los datos personales y las políticas y legislación al respecto, colaborando con las autoridades nacionales de la UE para garantizar la coherencia en la protección de datos. Así como, se ocupa de las reclamaciones y realiza investigaciones en base a las mismas.
C) Se hará cargo de las funciones de la secretaria del Comité Europeo de Protección de Datos, siendo responsable, en particular, de artículo 75, apartado 6, del Reglamento (UE) 2016/679: los asuntos corrientes del Comité; la comunicación entre los miembros del Comité, su presidente y la Comisión; la comunicación con

otras instituciones y con el público; la utilización de medios electrónicos para la comunicación interna y externa; la traducción de la información pertinente; la preparación y el seguimiento de las reuniones del Comité; y la preparación, redacción y publicación de dictámenes, decisiones relativas a solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Por último, el Supervisor Europeo de Protección de Datos será consultado por el Comité para elaborar y publicar, si procede, un memorando de entendimiento que determinará los términos de su cooperación y que será aplicable al personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento, artículo 75, apartado 4, del Reglamento (UE) 2016/679.

Capítulo 2. La Autoridad de control en los Estados Miembros

2.1. Naturaleza de la Autoridad de control

A efectos del Reglamento (UE) la Autoridad de control es la entidad, o varias entidades, designadas por los Estados Miembros de la UE, en los propios Estados Miembros, encargada de la supervisión de la aplicación, cumplimiento, del Reglamento y de su aplicación coherente en la UE, cooperando entre sí y con el Comité Europeo de Protección de Datos, artículo 51.1 y 51.2 del Reglamento (UE) 2016/679.

En función del artículo 51.1 del Reglamento (UE) 2016/679, el fin de la Autoridad de control es el de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

Cada Estado Membro tendrá una sola Autoridad de control que le represente en el Comité Europeo de Protección de Datos, siendo además la que garantice la coherencia con las además autoridades de control dentro del mismo Estado Miembro.

La Autoridad de control deberá gozar de la necesaria independencia, artículo 52 del Reglamento (UE) 2016/679, lo cual mediante la necesaria objetividad e imparcialidad pretende asegurar un control eficaz y fiable de la normativa de protección de datos[284].

Además, la Autoridad de control será nombrada con absoluta transparencia por uno de los siguientes sistemas: por el parlamento, por el gobierno, por el Jefe de Estado o un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros. El nombramiento se basará en los siguientes criterios: la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes, artículo 53 del Reglamento (UE) 2016/679.

2.2. Normas de establecimiento de la Autoridad de control. Reserva de Ley

El artículo 54 del Reglamento (UE) 2016/679, exige a los Estados Miembros que la regulación de su Autoridad de control se realice por medio de una ley. En este punto la UE aplica la reserva de ley, un mecanismo mediante el cual se ubica en el poder legislativo su regulación excluyendo intencionadamente a cualquier otro órgano de poder dentro de la Administración Pública.

La reserva de ley que exigen el Reglamento (UE), va más allá de las habituales reservas de ley obligando al Estado Miembro en determinadas materias.

En este orden de cosas, el artículo 54 del Reglamento determina que las leyes estatales que regulen a la Autoridad de control lo harán, como mínimo, en materia del establecimiento de cada Autoridad de control y las cualificaciones y en las condiciones de idoneidad necesarias para ser nombrado miembro de la misma, las normas y los procedimientos para el nombramiento del miembro o miembros, así como en la

[284] STJUE de 9 de marzo de 2010 (Gran Sala) (asunto C-518/07) apartado 25, p I-1910.

duración del mandato del miembro o los miembros, que no será inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la Autoridad de control por medio de un procedimiento de nombramiento escalonado.

En relación a los nombramientos las leyes estatales determinarán el carácter renovable o no del mandato del miembro o los miembros de cada Autoridad de control y, en su caso, el número de veces que podrá renovarse; así como las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada Autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

2.3. La Autoridad de control y el deber de secreto

El miembro o miembros y el personal de cada Autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

El secreto profesional ha sido tratado en el capítulo 5.5. del Título I, en esta Tesis. En este capítulo se analiza el amplio alcance del secreto profesional tal como lo entiende el ordenamiento jurídico español, apareciendo la figura del secreto profesional sobrevenido aplicable a cualquier persona que por su actividad tuviera conocimiento de un asunto íntimo y/o confidencial de cualquier persona.

2.4. Funciones de la Autoridad de control

Las funciones de cada Autoridad de control, en su territorio, vienen en el artículo 57 del Reglamento (UE) 2016/679. La primera función que tiene es la que emana de su propio nombre, la del control de la aplicación del Reglamento (UE) 2016/679 en el país de implantación, con especial atención cuando las actividades se dirijan a los niños.

Las funciones de la Autoridad de control se pueden clasificar en acciones o actividad de promoción, asesoramiento, ejercicio de la potestad administrativa y cooperación[285].

Las acciones de promoción incluyen la sensibilización tanto de los ciudadanos como de los responsables del tratamiento, promoviendo la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento, y de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento.

[285] AEPD (2019) "Funciones y poderes". Enero de 2019. Disponible en https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/funcion-y-poderes (28/02/2021).

La Autoridad de control también deberá alentar la elaboración de códigos de conducta y dictaminar y aprobar los códigos de conducta que den suficientes garantías y la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos.

Las actividades de asesoramiento se incluyen dentro de las funciones de la Autoridad de control, mediante asesoramiento tanto al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas, como a cualquier interesado en relación con el ejercicio de sus derechos en virtud del RGPD y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros, previa solicitud. También asesorará sobre las operaciones de tratamiento contempladas en la consulta previa. Hacer un seguimiento del desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales.

Las actividades de ejercicio de potestad administrativa engloban por una parte, la resolución de reclamaciones, es decir, tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación, por otra parte, llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra Autoridad de control u otra autoridad pública, así como, llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad.

Las autoridades de control también tendrán potestad sobre la autorización de las cláusulas contractuales y disposiciones a que se refiere el artículo 46, del Reglamento (UE), normas corporativas vinculantes de conformidad con el mecanismo de coherencia y cláusulas contractuales tipo para la contratación de los encargados del tratamiento.

Además, le corresponde a la Autoridad de control la revisión periódica de las certificaciones expedidas, acreditar a organismos de supervisión de los códigos de conducta, elaborar, mantener y publicar una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos y los criterios para la acreditación de organismos de supervisión de los códigos de conducta.

Por último, en cuanto a otras funciones de las autoridades de control, estas deberán cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento. En líneas generales, contribuir a las actividades del Comité Europeo de Protección de Datos y desempeñar cualquier otra función relacionada con la protección de los datos personales.

Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial[286].

[286] AEPD (6 Julio 2017) "Convenio de colaboración entre el Consejo General del Poder Judicial y la Agencia Española de Protección de Datos sobre colaboración en el ejercicio de las funciones propias de las autoridades de control en materia de protección de datos". Disponible en https://www.aepd.es/sites/default/files/2020-02/convenio-aepd-cgpj.pdf (28/02/2021) p 4.

2.5. Potestades de la Autoridad de control

Las potestades de la Autoridad de control atribuidas por el Reglamento (UE) 2016/679 son las que hacen referencia al poder de investigación, al poder sancionador y correctivo, al poder autorizador y a la acción consultiva. El ejercicio de los poderes conferidos a la Autoridad de control en virtud del Reglamento (UE) estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta, artículo 58 del Reglamento (UE) 2016/679.

Cada Estado miembro dispondrá por ley que su Autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

Las potestades de la Autoridad de control que asigna el Reglamento (UE) 2016/679 son la correctiva y sancionadora, la de autorización y la consultiva y la de investigación. Estas tres potestades se organizan:

I. Potestad de investigación indicados a continuación, artículo 58.1 del Reglamento (UE) 2016/679:
   a. Sancionar a todo responsable o encargado del tratamiento:
      - con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento,
      - con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento.
   b. Ordenar:
      - al responsable o encargado del tratamiento que
        – atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento,
        – las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado.
      - al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales,
      - la rectificación o supresión de datos personales o la limitación de tratamiento,
      - la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.
   c. Imponer:
      - una limitación temporal o definitiva del tratamiento, incluida su prohibición,

- una multa administrativa con arreglo al artículo 83 del Reglamento (UE), además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular.

d. Retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación.

II. Potestad de autorización y consultivos, artículo 58.3 del Reglamento (UE) 2016/679:

1. Autorizar:
   - el tratamiento de datos, si el Derecho del Estado miembro requiere tal autorización previa;
   - las cláusulas contractuales indicadas;
   - los acuerdos administrativos;
   - normas corporativas vinculantes de conformidad;
   - las cláusulas tipo de protección de datos.
2. Emitir
   - un dictamen y aprobar proyectos de códigos de conducta;
   - por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;
   - certificaciones y aprobar criterios de certificación.
3. Acreditar los organismos de certificación.
4. Asesorar al responsable del tratamiento conforme al procedimiento de consulta previa.

Cada Estado miembro podrá establecer por ley que su Autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del Reglamento (UE).

2.6. La Agencia Española de Protección de Datos

En España la Autoridad de control viene regulada en el Titulo VII, sobre autoridades de protección de datos, del artículo 44 a 62 de la Ley Orgánica 3/2018. Se regula la Agencia Española de Protección de Datos, artículo 44 a 56., regulando ese también las Autoridades Autonomías de Protección de Datos de los artículos 57 a 62.

También regula a la AEPD el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y por descontado por el Reglamento (UE) 2016/679 del parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a

la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

La Agencia Española de Protección de Datos, artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, es una autoridad administrativa independiente de ámbito estatal[287] con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones y tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia, artículo 44 de la Ley Orgánica 3/2018 [288].

El régimen jurídico de La Agencia Española de Protección de Datos se conforma de las siguientes normas: Reglamento (UE) 2016/679 del Parlamento 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; Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y sus disposiciones de desarrollo; y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto, artículo 45 de la Ley Orgánica 3/2018).

La Presidencia de la Agencia Española de Protección de Datos, y su Adjunto, serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos, previa publicidad en el Boletín Oficial del Estado de la convocatoria pública de candidatos, con dos meses de antelación.

La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta,

[287] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

[288] AEPD (6 Julio 2017) "Convenio de colaboración entre el Consejo General del Poder Judicial y la Agencia Española de Protección de Datos sobre colaboración en el ejercicio de las funciones propias de las autoridades de control en materia de protección de datos". Disponible en https://www.aepd.es/sites/default/files/2020-02/convenio-aepd-cgpj.pdf (28/02/2021).

por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

2.7. La Auditoría Preventiva en la Ley Orgánica 3/2108

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, desarrolla la Auditoria Preventiva en su artículo 54 sobre planes de auditoria, en su Sección 2.ª, de potestades de investigación y planes de auditoría preventiva, de su Título VII, sobre las autoridades de protección de datos.

La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII, de procedimientos en caso de posible vulneración de la normativa de protección de datos, y de los planes de auditoría preventivas, artículo 51 de la Ley Orgánica 3/2018.

En relación a los planes de auditoría preventiva la Ley Orgánica 3/2018, estipula en su artículo 55 de la Ley Orgánica 3/2018 los siguientes extremos:

1. Legitimidad. La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad.
2. Fin. Los planes de auditoría, tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de Ley Orgánica 3/2018, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.
3. Directrices. A resultas de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.
4. Colaboración. En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.
5. Obligado cumplimiento. Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría.

El Reglamento (UE) 2016/679 en su artículo 58.1.b) sobre los poderes de las autoridades de control, artículo 51 del Reglamento 2016/679 establece que cada Autoridad de control dispondrá de todos los poderes de investigación, llevando a cabo investigaciones en forma de auditorías de protección de datos.

2.8. La Autoridad Nacional de Seguridad para la Protección de la Información Clasificada. Una excepción

La Información Clasificada es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad, entendiéndose como información "todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma. La información puede estar clasificada en distintos grados en función del perjuicio que puede ocasionar su difusión no autorizada"[289].

En España los grados reconocidos de información clasificada son cuatro: secreto, reservado, confidencial y difusión limitada[290].

De esta forma en España y en el resto de países de nuestro entorno además de las Autoridades de Control en relación al RGPD existen otra autoridades de control de datos tales como las que controlan datos de información clasificada, que en España es la Autoridad delegada para la seguridad de la información clasificada, regulada por la Ley 9/1968, modificada por la Ley 48/78, sobre Secretos Oficiales, y su Decreto de desarrollo 242/1969 y por la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

[289] CNI Centro Nacional de Inteligencia. Oficina Nacional de Seguridad. Disponible en https://www.cni.es/es/ons/que_es_la_informacion_clasificada/ (28/02/2021).

[290] ONS (2018). "Normas de la Autoridad Nacional para la Protección de la Información Clasificada" Autoridad delegada para la seguridad de la información clasificada. Cuarta edición. NIPO: 083-19-040-0 (edición en línea) Disponible en https://www.cni.es/comun/recursos/descargas/DOCUMENTO_5_-_Normas_de_la_Autoridad.pdf (28/02/2021). p 27.

Capítulo 3. Responsable del tratamiento y encargado del tratamiento

3.1. Relevancia del responsable del tratamiento y del encargado del tratamiento

Las figuras del responsable del tratamiento y la del encargado del tratamiento son de extremada importancia tanto en el Reglamento (UE) 2016/679 como en la Ley 3/2018, sobre ellos recae toda la responsabilidad del tratamiento de datos y además la designación del delegado de protección de datos, artículo 37 del Reglamento (UE) 2016/679 y artículo 34 de la Ley 3 /2018.

Se puede decir que salvo la figura de la autoridad de protección de datos, nacional y autonómica, y la figura del Comité Europeo de Protección de Datos, todo el desarrollo del Reglamento (UE) 2016/679 recae sobre las figuras del responsable y del encargado del tratamiento.

Por otra parte, la figura operativa más relevante es la del delgado de protección de datos, designado bien por el responsable o bien por el encargado de protección de datos.

La Comisión Europea en una comunicación web explica lo que es un responsable y los que es un encargado del tratamiento. La web contiene una respuesta a una pregunta que realizan a la Comisión europea sobre "responsable o encargado del tratamiento en el Reglamento (UE) 2016/679"[291], que se traslada íntegramente a este documento:

> "El responsable del tratamiento determina los fines y los medios relacionados con el tratamiento de los datos personales. De modo que, si decide «por qué» y «cómo» deberán tratarse los datos personales, usted es el responsable del tratamiento. Los empleados que realizan el tratamiento de los datos personales en su organización lo hacen en cumplimiento de las funciones que usted ejerce como responsable del tratamiento.
>
> Usted será un corresponsable del tratamiento cuando, junto con una o más organizaciones, determine conjuntamente «por qué» y «cómo» deberán tratarse los datos personales. Los corresponsables del tratamiento deben concertar un acuerdo en el que se establezcan sus respectivas responsabilidades de cumplimiento con las normas del Reglamento general de protección de datos. Los principales aspectos del acuerdo deberán comunicarse a las personas sobre cuyos datos se realice el tratamiento.
>
> El encargado del tratamiento trata los datos personales únicamente por cuenta del responsable del tratamiento. El encargado del tratamiento de los datos suele ser un tercero externo a la empresa; sin embargo, en el caso de los grupos de empresas, una de ellas puede actuar como encargada del tratamiento para otra.
>
> Las obligaciones del encargado del tratamiento con respecto al responsable deberán especificarse en un contrato u otro acto jurídico. Por ejemplo, el contrato debe indicar lo que pasará con los datos personales una vez finalizado el contrato. Una actividad típica de los encargados es ofrecer soluciones informáticas, como almacenamiento en la nube. El encargado del tratamiento solo puede subcontratar una parte de esta tarea a otro

[291] COMISIÓN EUROPEA. "¿Qué es un responsable o encargado del tratamiento?" Web oficial de la Unión Europea. Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations /obligations/ controller-processor/what-data-controller-or-data-processor_es (28/02/2021).

encargado o designar un coencargado cuando haya recibido la autorización previa por escrito del responsable del tratamiento.

Existen situaciones en las que una entidad puede ser responsable o encargado del tratamiento, o ambas cosas.

Ejemplos

Responsable y encargado del tratamiento

Una cervecería que tiene muchos empleados firma un contrato con una empresa de nóminas, para poder pagarles los salarios. La cervecería indica a la empresa de nóminas cuándo deben pagarse las nóminas, cuándo un empleado abandona la empresa o si tiene un aumento de sueldo, y proporciona toda la demás información sobre la nómina y el pago. La empresa de nóminas proporciona el sistema informático y conserva los datos de los empleados. La cervecería es el responsable del tratamiento y la empresa de nóminas es el encargado del tratamiento.

Corresponsables del tratamiento

Su empresa presta servicios de guardería a través de una plataforma por internet. Al mismo tiempo, la empresa tiene un contrato con otra empresa que le permite ofrecer servicios de valor añadido. Esos servicios incluyen la posibilidad de que los padres no solo elijan la canguro, sino también que alquilen juegos y DVD que esta puede traer. Ambas empresas participan en los aspectos técnicos del sitio web. En este caso, las dos empresas han decidido utilizar la plataforma para ambos fines (servicios de guardería y alquiler de DVD o juegos) y a menudo compartirán los nombres de sus clientes. Por tanto, ambas empresas son corresponsables del tratamiento, porque no solo están de acuerdo en ofrecer la posibilidad de «servicios combinados», sino que también diseñan y utilizan una plataforma común.

Referencias

Artículo 4, apartados 7 y 8, y artículos 24, 26, 28 y 29; Considerandos 74, 79 y 81

Grupo de trabajo del artículo 29, WP 169. Dictamen 1/2010 sobre los conceptos de responsable y encargado" (Comisión Europea. Web oficial de la Unión Europea. "¿Qué es un responsable o encargado del tratamiento?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_es#respuesta (31/05/2020)

Tal como afirma la Comisión Europea el responsable del tratamiento es el que utiliza y maneja los datos o quien decide cómo se manejan o tratan, y en base a que criterio o fin[292]. En cambio, los encargados del tratamiento manejan o trata los datos como encargo o mandato del responsable del tratamiento.

La relación entre el responsable y el encargado del tratamiento nace única y exclusivamente de un acto jurídico, a ser posible de un contrato y mejor si es escrito, Artículo 28.1 del Reglamento (UE) 2016/679. La relación jurídica entre ambos es directa, de tal forma que para que el encargado pueda contratar con un tercero, subcontratar su tarea, deberá constar una autorización en el contrato entre el responsable y el

[292] STS 1280/2016 del 4 de abril de 2016 (Sala de lo Civil), FD 2º.

encargado. Esta autorización no podrá ser genérica sino deberá explicar el alcance de estas, objeto, causa y duración.

El Reglamento (UE) 2016/679 en su artículo 26.1 hace mención a los corresponsables del tratamiento cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. En este supuesto acordarán sus respectivas responsabilidades.

3.2. El responsable del tratamiento de datos en la normativa de protección de datos

En la Ley Orgánica 5 / 1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, aparece la expresión responsable del fichero, pero no responsable del tratamiento. Para esta disposición normativa responsable del fichero es toda persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en su artículo de definiciones, artículo 3, equipara al responsable del fichero con el responsable del tratamiento, diciendo "Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento", añadiendo a su vez que "Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

El Reglamento (UE) 2016/679 define al responsable del tratamiento en el artículo 4. 7) responsable del tratamiento o responsable:

> "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

Sobre el responsable recae el principio más relevante del RGDP, este es el principio de responsabilidad proactiva[293]. La AEPD entiende por este principio "la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento".[294]

El Reglamento (UE) 2016/679 dedica su Capítulo IV al responsable y al encargado del tratamiento, para lo cual no dedica ningún artículo para definir y describir al

[293] BUTTARELLI, G. (2016) "The EU GDPR as a clarion call for a new global digital gold standard". International. Data Privacy Law, Vol. 6 (2), 77-78. p 1.

[294] AEPD (2019) "Guía del Reglamento General de Protección de Datos. Para responsables del tratamiento". Guía de protección de datos UE. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/ guia-rgpd-para-responsables-de-tratamiento.pdf (31/01/2021). p 3.

responsable, sino que directamente en su artículo 24 se refiere a la "Responsabilidad del responsable del tratamiento". Sin tratar al responsable del tratamiento, describe al corresponsable del tratamiento en el artículo 26. Si bien luego, en el artículo 28 trata la figura del encargado del tratamiento. Para concluir, no trata la figura del responsable, pero si trata la figura del corresponsable y la del encargado.

La responsabilidad única del responsable en el tratamiento de los datos de las personas ha sido puesta de manifiesto por el Tribunal Supremo, incluso antes del año 2018, cuando ha defendido que los responsables deben responder de los daños y perjuicios causados por un tratamiento que no respete la normativa sobre protección de datos y carezca de cobertura jurídica[295].

Del texto del Reglamento (UE) se extrae en primer lugar, que el responsable puede ser bien una persona física, es decir, cualquier persona que trate con datos de personas, pero también puede ser el responsable del tratamiento cualquier persona jurídica, es decir, organización humana con fines conocidos, con plena capacidad de obra y con órganos de gobierno y dirección con competencias y potestades. No se le escapa a nadie, la complejidad de asignar responsabilidades a personas jurídicas, que sin duda corresponderán a quien ostente su representación legal, es decir, a sus administradores.

En segundo lugar, también la autoridad pública, un servicio u organismo público pueden instaurarse como responsables del tratamiento de datos. A lo cual hay que añadir que la responsabilidad del tratamiento puede recaer sobre una de las personas físicas y jurídicas mencionadas o sobre varias en conjunto.

En tercer lugar, se entiende que la persona jurídica puede tener naturaleza pública o naturaleza privada, y que nada impide que actúen conjuntamente en dicha responsabilidad.

El responsable del tratamiento aplicará, revisará y actualizará cuantas veces se requiera, las medidas técnicas y organizativas apropiadas a fin de cumplir el Reglamento. Aplicará políticas de protección de datos cuando la actividad del tratamiento o el tipo de dato así lo requieran. El responsable del tratamiento para demostrar el cumplimiento de sus obligaciones podrá utilizar la adhesión a códigos de conducta aprobados, artículo 40, o a un mecanismo de certificación aprobado, artículo 24 del Reglamento (UE) 2016/679.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales no tan solo no define lo que entiende por responsable del tratamiento, sino tampoco le dedica un artículo.

La Ley Orgánica 3/2018 entiende, en su artículo 33 dedicado al encargado del tratamiento, que quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679 tendrá

[295] STS 1280/2016 del 4 de abril de 2016 (Sala de lo Civil), FD 3º.

la consideración de responsable del tratamiento y no la de encargado. Aunque añade que esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público. En el mismo artículo 33 añade que tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

Estas dos normas, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, tratan al responsable y al encargado de forma distinta. Se puede afirmar que la descripción del responsable del tratamiento, en algunos aspectos, se hace diferidamente a través del articulado dedicado al encargado del tratamiento.

Resumiendo lo dicho en relación al responsable del tratamiento, se puede concluir que el responsable del tratamiento es el que ostenta la titularidad de la persona jurídica de la organización, o quién la representa, o la persona física que necesita los datos personales a tratar para cumplir sus fines y misión y/o el funcionamiento de su organización, de su negocio o de su proyecto de trabajo. Es responsable del tratamiento de datos aquel que los utilice para sus propios fines y que no sea en un entorno exclusivamente personal o doméstico, articulo2.2.c) del Reglamento (UE) 2016/679. Así pues, es el caso de una empresa, de un profesional o de un organismo público, tal es el caso de una unidad de la administración o de un organismo público con o sin personalidad jurídica propia. Finalmente, sobre el responsable del tratamiento recae el principio de responsabilidad proactiva.

3.2.1. El registro de actividades

El responsable del tratamiento de los datos y en su caso el encargado que haya contratado deberá llevar un registro, anotación o agenda de las actividades que realicen, sustituyendo a la inscripción de ficheros de la anterior LOPD 15/1999 no vigente.

Este registro deberá contener los siguientes campos e información, artículo 30 del Reglamento 2016/679[296]:

1. “el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable,
2. el nombre y los datos de contacto del delegado de protección de datos
3. los fines del tratamiento
4. una descripción de las categorías de interesados y de las categorías de datos personales
5. las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales
6. en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización

[296] AEPD (2018) “Elaborar el registro de actividades de tratamiento”. Diciembre 2018. Disponible en https://www.aepd.es/es/prensa-y-comunicacion/blog/elaborar-el-registro-de-actividades-de-tratamiento (28/02/2021).

internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo2, la documentación de garantías adecuadas

7. los plazos previstos para la supresión de las diferentes categorías de datos, cuando sea posible
8. una descripción general de las medidas técnicas y organizativas de seguridad, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
    a. la seudonimización y el cifrado de datos personales
    b. la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento
    c. la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico
    d. un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento"

La actividad del responsable del tratamiento de datos deberá centrarse en el registro de actividades de tratamiento, en primer lugar, revisando los tratamientos de datos llevados acabos en su establecimiento, en segundo lugar, anotar y estudiar las nuevas obligaciones que el Reglamento (UE) 2016/679 introduce y obliga al responsable del tratamiento. El responsable del tratamiento deberá revisar la estructura de los datos, los ficheros existentes, el nivel de detalle, la necesidad de minimizar o unificar en una única actividad de tratamiento de una misma finalidad o similares, legitimación, base jurídica o colectivo de afectados o interesados[297].

3.2.2. La protección del diseño

Concepto desarrollado por la Comisionada de Protección de Datos de Ontario, Ann Cavoukian, en la década de los 90. Fue presentado en la 31ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad del año 2009 como "Privacy by Design: The Definitive Workshop". Aceptado en la 32ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, en Jerusalén en el año 2010, con la aprobación de la "Resolución sobre la Privacidad por Diseño"[298].

[297] AEPD (2018) "Elaborar el registro de actividades de tratamiento". Diciembre 2018. Disponible en https://www.aepd.es/es/prensa-y-comunicacion/blog/elaborar-el-registro-de-actividades-de-tratamiento (28/02/2021).

[298] AEPD (2019) "Guía de privacidad del diseño". Noviembre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf (31/01/2021).

El diseño de los datos y los procedimientos de su tratamiento protegerán la privacidad de una forma decisiva y no deberá incorporarse como un añadido a posteriori[299].

El Considerando 78 del Reglamento (UE) 2016/679 entiende que las medidas técnicas y organizativas para garantizar el RPGD contempla también lo que viene a denominar, los principios de protección de datos desde el diseño y por defecto.

En cuanto "protección de datos desde el diseño y por defecto", el Considerando 78 del Reglamento (UE) 2016/679 describe:

1. "reducir al máximo el tratamiento de datos personales,
2. seudonimizar lo antes posible los datos personales
3. permitir a los interesados supervisar el tratamiento de datos
4. permitir al responsable del tratamiento crear y mejorar elementos de seguridad
5. desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que tengan en cuenta el derecho a la protección de datos cuando desarrollan y que se aseguren de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.
6. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."

El artículo 25, de protección de datos desde el diseño y por defecto, del Reglamento (UE) 2016/679 se dirige al responsable del tratamiento diciéndole que deberá aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, la minimización de datos y la integración de las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

El responsable del tratamiento garantizará que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad[300]. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles sin la intervención de la persona, a un número indeterminado de personas físicas, artículo 25.2 del Reglamento (UE) 2016/679. Este supuesto tiene un ejemplo muy visual, los archivos de historias clínicas de los hospitales con decenas de miles de documentos archivados y custodiados por los propios centros bajo la responsabilidad de los equipos directivos. En este supuesto, son varios los

[299] LLANEZA GONZALEZ, P. (2018) "Nuevo maco de cumplimiento en las obligaciones de protección de datos: la gestión de la privacidad desde la mitigación del Riesgo". Revista Privacidad y Derecho Digital, 11, 77-107, Año III. p 134.

[300] AEPD (2018) "Medidas de protección de datos desde el diseño y por defecto" de 27 de febrero de 2020. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/proteccion-de-datos-diseno-por-defecto (28/02/2021).

ejemplos de responsables que contratan al encargado para cumplir esta función del tratamiento de datos.

3.3. El encargado del tratamiento de datos en la normativa de protección de datos

En la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, no aparece la expresión encargado, ni encargado del tratamiento ni del fichero.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en su artículo de definiciones, artículo 3, define al encargado del tratamiento. En su punto g) dice: "Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales no define al encargado del tratamiento si bien le dedica el Titulo V, responsable y encargado del tratamiento. En dicho título el artículo 28 trata sobre las "obligaciones generales del responsable y encargado del tratamiento" y el artículo 33 regula el encargado del tratamiento. Del artículo 33 se desprende que encargado es quien accede al tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable[301].

Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado, artículo 28.1 Reglamento (UE) 2016/679.

En base al artículo 28 del Reglamento (UE) 2016/679, el tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) "tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público,
b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria,

[301] SAN 157/2018 de 12 de marzo de 2020 (Sala de la Contencioso), FD 5º.

c) tomará todas las medidas necesarias de conformidad con el artículo 32, de seguridad del tratamiento,

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento,

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III, sobre derechos del interesado,

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, de seguridad de los datos personales, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado,

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros,

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable."

La AEPD en septiembre de 2019, editó el modelo de Cláusula para contratos de encargados de tratamiento[302]. Este modelo incluye cláusula de confidencialidad y otra de protección de datos, además de las estipulaciones como encargado del tratamiento de datos y del sub-encargo de tratamiento asociados a subcontrataciones.

3.4. La seguridad de los datos

La AEPD, en su comunicado de 28 octubre de 2019, dice en relación a la importancia de las medidas de seguridad en las políticas de protección de datos que las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos[303].

La importancia a la que alude la AEPD se sustenta en el hecho de que no es verosímil asegurar el derecho fundamental a la protección de datos si no es a través de la aplicación de todas las medias razonables para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.

En este orden de cosas, la AEPD establece el criterio de "obligación de resultado" exigible por la jurisprudencia en relación a la obligación de establecer medidas de seguridad suficientes para impedir el acceso de datos de terceros[304].

[302] AEPD (2019) "Modelo de Cláusula para contratos de encargados de tratamiento". Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/clausulas-contratos-encargado-tratamiento.pdf (31/01/2021).

[303] AEPD (2019) "Análisis de riesgos y adopción de medidas de seguridad". Octubre 2019. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/analisis-de-riesgos (31/01/2021).

[304] Resolución de la Agencia Española de Protección de Datos R/00433/2018, de 10 de abril de 2018.

A su vez, la AEPD entiende que, para garantizar este nivel de seguridad exigible en estas tres vertientes de la seguridad, son necesarias medidas técnicas como organizativas[305].

El artículo 32, sobre seguridad del tratamiento, dentro la sección 2, de seguridad de datos, del capítulo IV, sobre el responsable del tratamiento y encargado del tratamiento, del Reglamento (UE) 2016/679 entiende que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta:

1. el estado de la técnica
2. los costes de aplicación
3. la naturaleza del tratamiento
4. el alcance del tratamiento
5. el contexto del tratamiento
6. los fines del tratamiento
7. los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas

El responsable y el encargado del tratamiento incluirán, entre otras, las siguientes medidas, artículo 32.1 Reglamento (UE) 2016/679:

1. la seudonimización y el cifrado de datos personales;
2. la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
3. la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
4. un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Todo ello nos conduce a que para establecer las medidas de seguridad el primer paso es la *evaluación del riesgo*, a través de la evaluación de impacto relativa a la protección de datos, artículo 35 Reglamento (UE) 2016/679, el segundo paso es disponer de forma efectiva las medidas de seguridad dirigidas a eliminar, o en su caso reducir, los riesgos para el tratamiento de los datos personales.

La Ley Orgánica 3/2018, en su Disposición adicional primera, sobre medidas de seguridad en el ámbito del sector público, determina que los responsables enumerados en el artículo 77.1 de esta Ley Orgánica deberán aplicar, a los tratamientos de datos personales, las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

[305] AEPD (2019) "Análisis de riesgos y adopción de medidas de seguridad". Octubre 2019. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/analisis-de-riesgos (31/01/2021).

Con carácter general, cualquier responsable del tratamiento de datos deberá vigilar y garantizar que no se producirán accesos no autorizados, a su vez, realizará copias de seguridad, realizará seudonimización y el cifrado de datos y realizará un control del almacenamiento, de los usuarios, de los soportes y del acceso a los datos.

A todo esto, hay que añadir que, además, el responsable del tratamiento de datos personales deberá informar que todo aquel que intervenga en la gestión o tratamiento de tus datos personales debe cumplir con el deber de secreto.[306]

3.5. Notificación de una violación de la seguridad de los datos personales

Una violación de la seguridad de los datos se produce cuando los datos sufren un incidente de seguridad que da lugar a la violación de la confidencialidad, disponibilidad o integridad de los datos, artículo 33 del Reglamento 2016/679.

Cuando se produce una violación de la seguridad de los datos personales cabe la posibilidad de que se puedan ver afectados los derechos y las libertades de la persona en relación a los derechos y libertades protegidas por el Reglamento (UE) 2016/679, es por este motivo por el cual se deberá notificar a la Autoridad de control sin demora y a más tardar 72 horas después de que hayan tenido constancia de ello[307].

La notificación a la Autoridad de control le corresponde al responsable del tratamiento, en el supuesto de que hubiera un encargado del tratamiento, este deberá notificar la violación de la seguridad de los datos al responsable del tratamiento[308].

Si la violación de la seguridad de los datos supone un alto riesgo para las personas afectadas, estas también deberán ser informadas, artículo 34 del Reglamento 2016/679. Le deberá informar el responsable del tratamiento. Ejemplo:

> "Un profesional de un hospital decide copiar la información de una serie de pacientes en un CD y la publica en internet. Los responsables del hospital se dan cuenta de esta situación varios días más tarde. En cuanto el hospital se da cuenta, el director del hospital tiene 72 horas para informar a la Agencia Española de Protección de Datos y también debe informar a los pacientes afectados. Si el hospital hubiera aplicado las medidas de protección apropiadas (como el cifrado de los datos), no existiría la probabilidad de que se concretizara el riesgo y podría quedar exento de notificarlo a los pacientes. Si los datos del paciente salen por internet identificados, es porque le hospital no tomo las medidas necesarias y en este caso deberá informar a los pacientes". (Comisión Europea. Web oficial de la Unión Europea.

[306] AEPD (2019) "Protección de Datos: Guía para el Ciudadano". Octubre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf (28/02/2021).

[307] COMISIÓN EUROPEA. Web oficial de la Unión Europea. "¿Qué es una violación de la seguridad de los datos y qué deberíamos hacer en caso de sufrir una?". Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_es (31/01/2021).

[308] Grupo de trabajo sobre protección de datos del artículo 29 "Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679" Adoptadas el 3 de octubre de 2017. Revisadas por última vez y adoptadas el 6 de febrero de 2018. Disponible en https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf (31/01/2021).

> "¿Qué es una violación de la seguridad de los datos y qué deberíamos hacer en caso de sufrir una?".[309]

La notificación contemplada en el apartado 1 del artículo 34 del Reglamento (UE) 2016/679, deberá contar, como mínimo, con:

> "a) la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) las posibles consecuencias de la violación de la seguridad de los datos personales; d) las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos."

3.6. La evaluación de impacto del Reglamento 2016/679

La Evaluación de Impacto en la Protección de Datos Personales (en adelante, la EIPD) es una herramienta, un proceso, con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.[310]

En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.[311]

La EIPD es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.

La Evaluación de Impacto en la Protección de Datos Personales está regulada en el Reglamento (UE) 2016/679 por el artículo 35, de la Sección 3, sobre la Evaluación de Impacto en la Protección de Datos Personales, y en la Ley Orgánica 3/2018 tan solo esta comentada de forma difusa en la redacción de algunos artículos.

La evaluación del Impacto, llevada a cabo por el responsable del tratamiento, de las operaciones de tratamiento en la protección de datos personales será necesaria cuando

[309] COMISIÓN EUROPEA. Web oficial de la Unión Europea. "¿Qué es una violación de la seguridad de los datos y qué deberíamos hacer en caso de sufrir una?". Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_es (31/01/2021).

[310] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021).

[311] COMISIÓN EUROPEA. Web oficial de la Unión Europea. "¿Qué es una violación de la seguridad de los datos y qué deberíamos hacer en caso de sufrir una?". Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_es (31/01/2021).

un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, artículo 35.1 del Reglamento (UE) 2016/679. También esta evaluación será necesaria cuando lo determine la Autoridad de control, artículo 35.4 del Reglamento (UE) 2016/679.

Deberá realizarse la evaluación del impacto de forma sistemática y exhaustiva de aspectos personales de personas físicas sometidas a un tratamiento automatizado, como la elaboración de perfiles y que produzcan efectos jurídicos para las personas físicas, artículo 35.3.a) del Reglamento (UE) 2016/679.

También se realizará la evaluación en tratamientos a gran escala de las categorías especiales de datos del artículo 9.1 o de los datos personales relativos a condenas e infracciones penales del artículo 10, ambos del Reglamento (UE) 2016/679, artículo 35.3.b) del Reglamento (UE) 2016/679, y en observaciones sistemáticas a gran escala de una zona de acceso público, artículo 35.3.c) del Reglamento (UE) 2016/679.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, prácticamente no hace referencia alguna a la EIPD. Sin embargo, hace las siguientes menciones:

1. Los obligados. En el artículo 28 sobre las obligaciones generales del responsable y encargado del tratamiento, del capítulo "Disposiciones generales. Medidas de responsabilidad activa", del TÍTULO V, sobre el responsable y encargado del tratamiento, dice que los responsables y encargados, artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.
2. Los riesgos de la reidentificación. En la Disposición adicional decimoséptima relativa a tratamientos de datos de salud, en su apartado 2 sobre los criterios que deberá seguir el tratamiento de datos en la investigación en salud, en su punto f) dice que cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a: 1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la Autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

En consecuencia, la Ley 3/2018, identifica sobre quien recae la responsabilidad de los EIPD y resalta su importancia en los estudios de investigación de salud y en especial en los riesgos de la reidentificación como consecuencia de la anonimización o seudonimización de los datos.

3.6.1. El proceso de Evaluación del Impacto en la Protección de Datos Personales (primera fase de EIPD)

Para elaborar una EIPD, se debe disponer de una metodología que considere los requerimientos exigidos por el Reglamento (UE) 2916/679 en su artículo 35.7, donde se establece que la EIPD deberá incluir como mínimo:

a. Una descripción sistemática de la actividad de tratamiento previstas.
b. Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.
c. Una evaluación de los riesgos.
d. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad.
e. Mecanismos que garanticen la protección de datos personales.

En esta evaluación se debe empezar en primer lugar, por describir el ciclo de vida de los datos. Descripción detallada del ciclo de vida y del flujo de datos en el tratamiento. Identificación de los datos tratados, intervinientes, terceros, sistemas implicados y cualquier elemento relevante que participe en la actividad de tratamiento, artículo 35.7.a) del Reglamento (UE) 2016/679. En segundo lugar, analizar la necesidad y proporcionalidad del tratamiento. Análisis de la base jurídica para la legitimación de terceras personas, la finalidad y la necesidad y proporcionalidad del tratamiento que se pretenden llevar a cabo, artículo 35.7.b) del Reglamento (UE) 2016/679.

Una vez contextualizado el tratamiento de los datos, viendo la esencia de los datos, naturaleza, tipo de dato, categoría, fin de cada uno de ellos, captura, recolección, utilidad, manejo, almacenamiento, repositorio, acceso, agentes o personas que vayan a utilizar o a acceder al dato, tiempo de utilidad y destrucción, se debe pasar a la fase de analizar los riesgos que conlleva cada uno de los pasos del tratamiento para garantizar los principios y derechos del Reglamento (UE) 2016/679.

El obligado a realizar el EIPD es el responsable del tratamiento, no es el delegado de protección de datos. El artículo 35.2 del Reglamento (UE) 2016/679 dice: “El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos”, artículo 35.2 del Reglamento (UE) 2016/679.

Por tanto, el delegado de protección de datos (en adelante DPO) proporciona el asesoramiento necesario al responsable del tratamiento. Es importante destacar que el DPO no es en todos los casos una figura de obligado nombramiento. El RGPD establece los supuestos en los cuales se considera obligatorio disponer de DPO.

Según la AEPD[312], las organizaciones que llevan a cabo tratamientos que, por su número o por sus características, impliquen un cierto grado de complejidad, deberían contar con el asesoramiento técnico adecuado para estar en condiciones de cumplir con el Reglamento (UE) 2016/679 y poder demostrarlo. Por ello, resultaría recomendable que estas organizaciones designen un responsable de protección de datos que pueda proporcionar este asesoramiento. Si esta figura reúne las condiciones que el Reglamento (UE) 2016/679 establece para los DPO, las organizaciones podrán beneficiarse de los incentivos previstos en el Reglamento (UE) 2016/679 y en la legislación española.

En el caso de que el responsable del tratamiento esté adherido a algún código de conducta, artículos 40 y siguientes del Reglamento (UE) 2016/679, donde se incluya una metodología propia, se puede utilizar la misma para la realización de las EIPD sin eximir de la obligación de realizar la EIPD si fuese de aplicación.

3.6.2. Análisis de riesgos (segunda fase de EIPD)

El análisis de riesgo constituye la segunda fase del proceso de la evaluación del impacto en protección de datos personales.

La Real Academia Española define como riesgo a la contingencia o a la proximidad de un daño. Por otra parte, también se entiende por riesgo a una medida de peligrosidad. Esta medida pondera la magnitud de un daño o lesión frente a una situación peligrosa, o situación con capacidad de producir daño, asumiendo vulnerabilidad, o probabilidad de que ocurran daños frente a un peligro o frente a una situación con posibilidad de causar un daño o lesión[313].

El peligro o la posibilidad de causar un daño no está solo vinculado a la situación principal sino a las situaciones que rodean a la principal o al entorno. Siempre cabe la posibilidad de que la causa del daño haya sido fortuita e incluso imprevisible u oculta.

La existencia de riesgo en cualquier actividad humana y en especial en aquellas que comportan un servicio provisto a terceros, requiere una gestión de los mismos. La norma ISO 31000, sobre gestión de riesgos en su revisión de 2009, propone un estándar de gestión, si bien la norma ISO 27001, en revisión de 2013, ofrece requisitos para la Gestión de la Seguridad de la Información y la norma ISO 9001, en revisión de 2015, lo hace en el contexto de Sistema de Gestión de la Calidad.

La diferencia principal entre la EIPD y los análisis de riesgos tradicionales reside en que la EIPD se realiza desde "el punto de vista del interés del sujeto" mientras que los análisis de riesgos se realizan desde el punto de vista del "riesgo para la entidad".

[312] AEPD (2018) "¿Qué es un delegado de protección de datos?" Diciembre 2018. Disponible en https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-un-delegado-de-proteccion-de-datos (31/01/2021).

[313] OLMEDILLA ZAFRA, A., CARMEN GARCÍA MONTALVO, C., MARTÍNEZ SÁNCHEZ, F. (2006) "Factores psicológicos y vulnerabilidad a las lesiones deportivas: un estudio en Futbolistas". Revista de Psicología del Deporte (Universitat de les Illes Balears. Universitat Autónoma de Barcelona) Vol. 15, 1, 37-52. p 39.

El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados en relación con los derechos y garantías del Reglamento (UE) 2016/679 y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable. Esto implica iniciar el análisis del riesgo ya en desde el diseño, entre lo que incluimos los procesos de contratación de determinados soportes para el tratamiento de datos como puede ser los sistemas informáticos[314].

El análisis de riesgo es la segunda fase de evaluación de impacto relativa a la protección de datos del Reglamento (UE) 2016/679, artículo 35.7.c) del Reglamento (UE) 2016/679. Asegurar la correcta identificación de los riesgos a los que están expuestas las actividades de tratamiento es una parte clave para poder realizar una evaluación completa. La no identificación de riesgos implica que estos no se evalúan y no se tratan, y el tratamiento podría estar más expuesto al potencial riesgo.

Cuando sea probable que un tipo de tratamiento en particular, si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

En base a la Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos (en adelante también GPEIPD) de la AEPD, sujetas al Reglamento General de Protección de Datos, Reglamento (UE) 2016/679, cabe mencionar:

- "La evaluación de riesgos consiste en valorar y estimar la probabilidad y el impacto de que el riesgo se materialice.
- Definir el criterio que se seguirá a la hora de valorar los riesgos. Los criterios para cuantificar los riesgos, estimar el nivel de impacto y su probabilidad, se pueden basar en estándares o se pueden definir a criterio de la organización.
- El riesgo inherente es el riesgo intrínseco de cada actividad. El riesgo inherente surge de la exposición que se tenga a la operación de tratamiento en particular y de la probabilidad de que la amenaza asociada al riesgo se materialice.
- Metodología ISO 29134 de valoración de la probabilidad de riego e impacto basada en cuatro niveles:
    a. Probabilidad despreciable: muy baja o forma fortuita
    b. Probabilidad limitada: es baja u ocasional
    c. Probabilidad significativa: alta o con bastante frecuencia
    d. Probabilidad máxima: muy elevada o con mucha frecuencia

  El impacto también se evaluará con la misma escala de cuatro valores posibles:
    a. Impacto despreciable: muy bajo o prácticamente despreciables

[314] DROUGKAS, A. LIVERI, D. ZISI, A. KYRANOUDI P. (febrero de 2020) "Cloud security for Healthcare sercices". European Unión Agency Cibersecurity. Disponible en https://www.enisa.europa.eu/ publications/report-files/translation-procurement-guidelines-for-cybersecurity-in-hospitals/ procurement-guidelines- full-version-es.pdf (30/04/2021). p 30.

b. Impacto limitado: es bajo o sin impacto relevante
c. Impacto significativo: alto o elevado
d. Impacto máximo: muy alto

- Para evaluar el impacto asociado a un riesgo, se recomienda realizar la evaluación considerando tres dimensiones diferentes de posibles daños que se pueden producir sobre el interesado:
  1. Daño físico: Conjunto de acciones que pueden ocasionar un daño en la integridad física del interesado.
  2. Daño material: Conjunto de acciones que pueden ocasionar pérdidas económicas, de patrimonio, de empleo, etc.
  3. Daño moral: Conjunto de acciones que pueden ocasionar un daño moral o mental en el interesado, como una depresión, fobias, acoso, etc.
- La escala de impacto dependerá del tipo y cantidad de daño o perjuicio causado. El valor final de impacto deberá ser solo uno por riesgo, entre las cuatro posibilidades: despreciable (1), limitado (2), significativo (3) y máximo (4)
- La matriz de riesgo se forma relacionando probabilidad e impacto:

  Asignado un valor a la probabilidad y otro valor al impacto, se obtiene una matriz de riesgos que se corresponde con el riesgo inherente resultado de aplicar la fórmula de estimación del riesgo.

  El resultado del riesgo inherente se puede considerar en los siguientes niveles en función del valor obtenido."

Adaptación tabla de la Guía práctica para Las evaluaciones de impacto en la protección de los datos sujetas al RGPD[315]:

Tabla 5. Adaptación de tabla de GPEIPD de la APED (adaptación de elaboración propia)

	Impacto	Despreciable	Limitado	Significativo	Alto
Probabilidad		1	2	3	4
Despreciable	1	1	2	3	4
Limitado	2	2	4	6	8
Significativo	3	3	6	9	12
Máximo	4	4	8	12	16

[315] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021). p 29.

La Agencia Española de Protección de Datos en su Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD, presenta un ejemplo de cálculo de riesgo inherente que se traslada a estas páginas.

> "Ejemplo:
>
> Para poder estimar y valorar el riesgo, es necesario tener contexto sobre la exposición a la que se somete el riesgo.
>
> Para dotar de contexto al ejemplo, supongamos una aplicación móvil con almacenamiento en la nube que captura datos a través de weareables (dispositivos como un reloj o pulsera), además de permitir la introducción manual de datos de salud por parte del usuario.
>
> La finalidad de la actividad de tratamiento es monitorizar la actividad del usuario y recomendar hábitos de vida saludables. La aplicación móvil no dispone de medidas de control de acceso, ni de detección de malware, además no se realizan copias de seguridad de los datos. "

Adicionalmente, durante la fase de registro del usuario no se solicita consentimiento expreso para ninguna finalidad adicional a la mencionada. Ante este contexto, se puede identificar, entre otras, varias amenazas y riesgos asociados que se describen y evalúan a continuación:

Tabla 6. Guía práctica para Las evaluaciones de impacto en la protección de los datos sujetas al RGPD[316]

Tipo de amenaza	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo inherente
Acceso ilegitimo a los datos	Fuga de información (derivada de la pérdida del dispositivo móvil)	Acceso no autorizado por parte de terceros a datos de salud (violación de la confidencialidad)	Significativo (3)	Significativo (3)	Alto (9)
	Operación de tratamiento no autorizada (derivada del uso de los datos para una finalidad sin base legitimadora, por ejemplo, acciones de marketing indirecto sobre productos de salud)	Uso ilegítimo de datos personales (vulneración de los derechos y libertades)	Máxima (4)	Limitado (2)	Alto (9)
Modificación no autorizada de los datos	Ataque cibernético (malware que modifica los datos almacenados en la nube)	Modificación de datos no autorizada por parte de terceros (violación de la integridad)	Significativa (3)	Limitada (2)	Media (6)
	Operación de tratamiento no autorizada (derivada de una decisión automatizada en base al perfilado de datos erróneo por una mala programación del software, por ejemplo, una categorización de personas saludables con acceso a determinadas coberturas de un seguro de salud)	Uso ilegítimo de datos personales (vulneración de los derechos y libertades)	Máxima (4)	Significativa (3)	Muy alta (12)
Eliminación de los datos	Corte de suministro eléctrico o fallos en servicios de comunicaciones (como consecuencia del fallo se produce un periodo temporal en el cual los datos no han sido almacenados)	Pérdida de datos almacenados en el sistema (violación de la disponibilidad)	Limitada (2)	Limitada (2)	Media (4)
	Ataque intencionado que provoca la indisponibilidad de los datos (como consecuencia de un ataque de cifrado de las bases de datos que inhabilita las mismas)	Pérdida de datos almacenados en el sistema (violación de la disponibilidad)	Significativa (3)	Significativa (3)	Alto (9)

[316] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021). p 30.

3.6.3. Propuestas, medidas o respuestas a adoptar en base a los riesgos (tercera fase de EIPD)

La propuesta de medidas constituyen la tercera fase del proceso de la evaluación del impacto en protección de datos personales.

En la EIPD tras el análisis de riesgo cabe abordar la fase siguiente dentro del proceso de gestión de riesgos. Esta tercera fase se encarga de determinar la respuesta o las medidas para tratar el riesgo y reducir el nivel de exposición al peligro, es decir, reducir la vulnerabilidad, artículo 35.7.c) del Reglamento (UE) 2016/679.

Dentro de la ISO 31000 se completan cinco fases: la fase de identificación y evaluación, las hemos tratado en el apartado anterior; las fases de tratamiento, monitorización y comunicación, que se tratan en esta segunda fase del EIPD.

Es importante destacar que el objetivo principal de una EIPD no es eliminar completamente el riesgo asociado a las actividades de tratamiento, lo que se pretende es reducir el mismo hasta un nivel aceptable para poder llevar a cabo estas actividades garantizando los derechos y libertades de los interesados.[317]

Una vez conocidas las amenazas y las debilidades del tratamiento de datos es preciso analizar las opciones de la gestión de esas amenazas y debilidades en cuanto a su efectividad y en cuanto a la balanza de beneficios y coste y los riesgos de su implementación. Las opciones de tratamiento de riesgos según ISO 31000:2018 no son excluyentes entre sí y pueden incluir una o varias de las siguientes acciones[318]:

- Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.
- Adoptar acciones para disminuir la probabilidad del riesgo.
- Implementar acciones que disminuyan el impacto negativo del riesgo.

El tratamiento de riesgos según ISO 31000:2018 aunque se diseñe e implemente en forma cuidadosa, puede no ofrecer los resultados esperados para la organización o para algunas partes interesadas. Por ello, el monitoreo y la revisión deben formar parte integral del proceso de tratamiento de riesgos a fin de garantizar que las acciones implementadas sigan siempre siendo efectivas y seguras.

[317] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021). p 4.

[318] ESCUELA EUROPEA DE EXCELENCIA (31 mayo 2018). "Cómo realizar el tratamiento de riesgos según ISO 31000:2018". Disponible en https://www.escuelaeuropeaexcelencia.com/ 2018/05/ como-realizar-el-tratamiento-de-riesgos-segun-iso-310002018/ (31/05/2020).

La Agencia Española de Protección de Datos, plantea cuatro medidas para gestionar el riesgo: reducir, retener, transferir o anular el riesgo. A tenor literal la AEPD describe las siguientes medidas[319]:

a. "Reducción del riesgo: para reducir el nivel de riesgo, se deben establecer medidas de control que reduzcan los niveles de probabilidad y/o impactos asociados al riesgo inherente.
b. Retención del riesgo: si el nivel de riesgo inherente es inferior al nivel de riesgo considerado como aceptable, no existe necesidad de implementar controles adicionales.
c. Transferencia del riesgo: consiste en compartir un riesgo con una organización externa. Se puede transferir el riesgo a una aseguradora que afronte las posibles consecuencias materiales. Sin embargo, se ha de considerar que, en ocasiones, la transferencia de riesgos puede generar otros riesgos. Por ello, la transferencia puede generar la necesidad de análisis adicionales.
d. Anulación del riesgo: si el riesgo es muy elevado y no se quiere asumir el mismo, se puede decidir abandonar la actividad de tratamiento."

Adicionalmente a las medidas para tratar el riesgo se dispone de las medidas de control que tienen como objetivo mitigar o minimizar el riesgo asociado a una operación de tratamiento. Durante el proceso de definición de las medidas de control se debe considerar de forma independiente cada riesgo identificado y establecer tantas medidas de control como sean necesarias hasta lograr un nivel de riesgo aceptable. Existen las medidas de control organizativas, legales, técnicas, etc.

Una vez se hayan aplicado las medias de control para mitigar el riesgo, queda por considerar el riesgo residual[320]. A diferencia del riesgo inherente, el riesgo residual contempla las medidas de control definidas sobre la actividad de tratamiento para valorar la probabilidad y/o el impacto asociado al riesgo[321]. Para evaluar el riesgo residual, se debe estimar de nuevo la probabilidad y el impacto considerando las medidas de control definidas.

La GPEIPD presenta un ejemplo de medida de control. Ante un riesgo de acceso no autorizado por parte de terceros en un proceso de autenticación, el hecho de establecer un usuario y una contraseña asignados al usuario, cumplimiento con políticas de control de acceso e identificación, reduce significativamente la probabilidad de que un tercero

[319] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021). p 31.

[320] GARCIA-LEON, FJ. et Al (2020) "La evaluación de impacto en protección de datos en los proyectos de investigación". Gaceta Sanitaria. 34(5), 521–523. Disponible en https://reader.elsevier.com/reader/sd/pii/ S0213911119302675?token= C5CE040986C46130913021 C379F1DFA C33A700468EA302 9465 A13 0FC1 C8A4B8B0BC92C4A523EAA799B4BC5AB51E9F35B (28/02/2021). p 522.

[321] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021). p 32.

pueda realizar un acceso no autorizado. En este caso, la medida de control reduce la probabilidad de riesgo y, por tanto, minimiza el riesgo residual asociado.

Ejemplo práctico de estimación del riesgo residual:

- Ciclo de vida del dato (fase almacenamiento): Almacenamiento de datos de clientes en dispositivos móviles.
- Amenaza: pérdida del dispositivo móvil.
- Riesgo: acceso no autorizado por parte de terceros a datos de salud (violación de la confidencialidad).
- Impacto: violación de derechos fundamentales (Significativo).
- Probabilidad: se puede producir cada vez que el usuario no tiene en su poder el dispositivo móvil (Significativa).
- Riesgo inherente: impacto x Probabilidad x = (Riesgo alto).
- Medidas de control: método de autenticación mediante usuario, contraseña y huella biométrica. Cifrado del dispositivo móvil y seudonimización de los datos.
- Eficacia del control: reduce la probabilidad a despreciable, debido a que, aunque se pierda el dispositivo, no será posible el acceso sin credenciales. Adicionalmente, reduce el impacto a despreciable, debido a que, aunque se pierda el dispositivo, los datos nunca serán identificables evitando producir daños sobre los interesados.
- Riesgo residual: impacto x probabilidad x = (Riesgo bajo).

3.6.4. Plan de acción (cuarta fase de EIPD)

La elaboración del plan de acción constituye la cuarta fase del proceso de la evaluación del impacto en protección de datos personales.

Se debe elaborar un plan de acción donde se describan todas las medidas de control definidas para tratar los riesgos identificados y concluir con respecto al resultado obtenido. Este Plan de Acción se acopla como una tercera fase.

Un plan de acción es el conjunto de iniciativas que se deben llevar a cabo para implantar los controles que ayudan a reducir el riesgo de una actividad de tratamiento hasta un nivel considerado aceptable. Se recomienda que el plan de acción incluya al menos los siguientes campos de información[322]: el control, la descripción del control, el responsable de implantación y el plazo de la implantación.

Para la ejecución del plan de acción, se deben considerar dos posibilidades:

[322] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021). p 33.

1. La EIPD se ha hecho sobre un nuevo tratamiento: el plan de acción obtenido se deberá considerar durante la fase de definición de requerimientos de la actividad de tratamiento (privacidad desde el diseño).
2. La EIPD sobre un tratamiento ya existente: lanzar un proyecto o iniciativa para implantar las medidas incluidas en el plan de acción sobre el tratamiento actual.

En base al GPEIPD de la AEPD el responsable del tratamiento debe establecer un plazo máximo en el cual se deben implantar las medidas de control. En caso de superar el plazo establecido, si el riesgo residual actual del tratamiento no será aceptable, el responsable del tratamiento puede exigir que se interrumpa el tratamiento hasta la implantación de las medidas correspondientes.

La conclusión de la EIPD debe realizarse basándose en el nivel de riesgo residual obtenido durante la fase de gestión de riesgos, valorando si este es elevado o se considera aceptable y dentro de unos límites razonables. Escenarios posibles, el favorable y el desfavorable, se describen de la siguiente forma[323]:

A. No es favorable: se debe analizar la posibilidad de incluir medidas de control adicionales, disminuyendo el riesgo hasta un nivel aceptable. Si no fuese posible el tratamiento no se podría llevar a cabo y sería necesario activar el procedimiento de consulta previa a la Autoridad de control.
B. Es favorable: la actividad de tratamiento se puede llevar a cabo, siempre y cuando, las medidas de control incluidas en el plan de acción hayan sido implantadas.

Como criterio general, siempre y cuando el resultado de la EIPD suponga que el riesgo residual del tratamiento es alto o muy alto, el responsable del tratamiento debe realizar una consulta a la Autoridad de control, artículo 36 del Reglamento (UE) 2016/679. La consulta a la Autoridad de control, artículo 36, apartado 3, del Reglamento (UE) 2016/679, deberá incluir la siguiente información:

- "Las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento
- Los fines y medios del tratamiento previsto
- Las medidas y garantías establecidas para proteger los derechos y libertades de los interesados
- Los datos de contacto del DPO
- La EIPD
- Cualquier otra información que solicite la Autoridad de control"

[323] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021). p 34.

Por defecto, la EIPD debe contener toda la información requerida por el RGPD, por tanto, debe ser suficiente con entregar la EIPD, la metodología aplicada y una explicación de cómo se ha llevado a cabo.

Es fundamental que se realicen las fases de monitorización y comunicación (ISO 31000), una adecuada supervisión y una posterior revisión de la implantación de las medidas de control definidas en la EIPD para reducir el riesgo inherente hasta un riesgo residual que permita llevar a cabo el tratamiento garantizando los derechos y libertades de las personas físicas. A nivel práctico, es recomendable que una figura delegada supervise y garantice que las medidas de control definidas durante la EIPD se implanten adecuadamente antes de llevar a cabo las actividades de tratamiento de datos de carácter personal por parte del responsable del tratamiento (GPEIPD de la AEPD).

En ningún caso se puede proceder a llevar a cabo el tratamiento si el riesgo es elevado. En aquellos casos donde la EIPD se concluya con un riesgo residual elevado, el responsable del tratamiento deberá activar el procedimiento de Consulta Previa a la Autoridad de control local. En función de la resolución a la que llegue la Autoridad de control, se establecerán las condiciones y medidas que se deben aplicar para llevar a cabo el tratamiento o, si fuese posible su aplicación, se indicaría que en ningún caso se podrá llevar a cabo el tratamiento. De igual modo, si la Autoridad de control especificara una serie de medidas para poder realizar el tratamiento, será necesario realizar y planificar un plan de acción para implantarlas y re-evaluar su impacto en el cálculo del riesgo residual futuro [324].

3.6.5. Mapas de riesgos

La identificación de riesgos permite la construcción de mapas de riesgos: son métodos de prevención que detectan los riesgos y amenazas para la actividad humana.

Un mapa de riesgos es una herramienta, basada en los distintos sistemas de información, que pretende identificar las actividades o procesos sujetos a riesgo, cuantificar la probabilidad de estos eventos y medir el daño potencial asociado a su ocurrencia[325].

El concepto de mapa de riesgo engloba cualquier instrumento informativo que, mediante informaciones descriptivas e indicadores adecuados, permita el análisis periódico de los riesgos. La lectura crítica de las informaciones sintéticas que se originan, debe permitir la programación de planes de intervención preventiva y la verificación de su eficacia[326].

[324] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021). p 37.

[325] RODRÍGUEZ LÓPEZ. M. ET AL. (2013) "Mapa de Riesgos: Identificación y Gestión de Riesgos" Finanzas y Sistemas de Información para la Gestión (FYSIG), 2 (1), 1-29. p 3.

[326] GARCÍA GÓMEZ MM. (1994) "Los mapas de riesgos. Concepto y metodología para su elaboración" Rev. San.Hig. Pub, 68 (4), 443-453. p 448.

Los mapas de riesgos no vienen reflejados ni en el Reglamento (UE) 2016/679 ni en la Ley Orgánica 3/2018. Si embargo, en el ordenamiento jurídico español es abundante la referencia de elaboración de mapas de riesgos en los procesos de análisis y evaluación de riesgos. Como muestra de ello se traen los siguientes ejemplos:

1. mapa de riesgos para la seguridad del paciente[327],
2. mapas de riesgos laborales[328],
3. mapa de riesgos de procesos[329],
4. mapa de riesgo químico[330],
5. mapas de riesgos en el contexto de la ONU[331].

La AEPD entiende que la Evaluación de Impacto es un proceso que no se agota cuando se ha finalizado. Los responsables, y así lo señala el propio RGPD, deberían revisar si los tratamientos siguen siendo conformes con la Evaluación a la que hubieran sido sometidos y, en todo caso, hacerlo cuando exista un cambio del riesgo del tratamiento. En este orden de cosas hay mucha similitud entre lo que la norma denomina Evaluación del Impacto con los tradicionales Mapas de Riesgo.

3.7. La consulta previa en el Reglamento 2016/679

Es una medida que corresponde tomar, en su caso, al responsable del tratamiento.

El responsable consultará a la Autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 del Reglamento (UE) 2016/679 muestre que el tratamiento entrañaría un riesgo o un alto riesgo si el responsable no toma medidas para para mitigarlo, artículo 36 del Reglamento (UE) 2016/679[332].

Los Estados miembros deberán consultas a la Autoridad de control durante la elaboración de toda propuesta legislativa que haya de adoptar un Parlamento nacional,

[327] MARQUÉS RACIONERO MJ ET AL. (2012) "Guía de elaboración de mapa de riesgos" EnfermNefrol vol.15(1) 176-177. p 177.

[328] Artículo 10.b) de la Ley31/1995. de 8 de noviembre, de Prevención de Riesgos Laborales.

[329] SERGAS. Consejería de Saude (2015). (2014) "Sistema de Seguridad del Paciente y Gestión de Riesgos Sanitarios". Servicio Gallego de Salud. Xunta de Galicia. Disponible en https://www.sergas.es/Calidade-e-seguridade-do-paciente/ Documents/ 6 /SISTEMA%20SEGURIDAD%20DEL% 20PACIENTE%20Y% 20GESTION %20 DE% 20REISGOS-SERGAS_castellano.pdf.

[330] FERRÓN VIDÁN, L. (2014) "Mapa de riesgo químico". ISSGA. Instituto Gallego de Seguridad y Salud Laboral Sector Industrial. Xunta de Galicia. Santiago de Compostela. Disponible en http://issga.xunta.gal/export/sites/default/recursos/descargas/documentacion/publicacions/MRQ_CAS_20140604_DEF_WEB.pdf (31/01/2021).

[331] PICARD M. (2014) "Leyes y reglamentos eficaces para la reducción del riesgo de desastres: Informe multinacional". PNUD. Naciones Unidas. ONU. Federación internacional de sociedades de la Cruz Roja y de la Media Luna Roja. Disponible en https://www.undp.org/content/dam/undp/library/ crisis%20prevention/ UNDP_CPR_DRRLaw_Spanish_Aug2014.pdf (31/01/2021).

[332] AEPD (2021) "Formulario de Consulta Previa". Disponible en https://sedeagpd.gob.es/sede-electronica-web/vistas/formConsultaPrevia/procedimientoConsultasPrevias.jsf. (31/01/2021)

o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento, artículo 36.4 del Reglamento (UE) 2016/679.

Los efectos de la consulta previa, frente a tratamientos no ajustados al Reglamento:

- la Autoridad de control deberá asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58 (Poderes). Plazos: ocho semanas desde la solicitud de la consulta, con prorroga de seis semanas.

El Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la Autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública, artículo 36.5 del Reglamento (UE) 2016/679.

La Ley Orgánica 3/2018 hace referencia a la consulta previa cuando habla de las obligaciones de los responsables y encargados del tratamiento, al mismo tiempo que hace referencia a los EIPD, artículo 28 de la Ley Orgánica 3/2018.

Capítulo 4. Delegado de protección de datos

4.1. El delegado de protección de datos

Los elementos clave de la nueva legislación después del principio de proactividad y del principio de protección pasiva[333] son, por una parte, el reforzamiento del consentimiento del interesado y, por otra parte, la creación de la figura del delegado de protección de datos (DPO).

El primer antecedente de esta figura se encuentra en la legislación alemana federal sobre protección de datos del año 1997[334], en su sección 38 sobre Oficial de protección de datos de organismos no públicos, determina que el responsable o el encargado (controlador y procesador) designará un oficial de protección de datos o un oficial de protección de datos en organizaciones con al menos a 20 empleados o trabajadores en procesamientos automatizados de datos personales. Regula en los artículos 5 a 7, 0ficiales de protección de datos de organismos públicos. El segundo antecedente se encuentra en la Directiva 95/46/CE bajo en nombre de "encargado de protección de datos", artículo 18 sobre Obligación de notificación a la Autoridad de control, de la Directiva 95/46/CE del Parlamento y del Consejo de 24 de octubre de 1995.

Esta nueva figura está vinculada al responsable del tratamiento o al encargado del tratamiento, dos figuras, estas últimas, insuficientemente definidas en el Reglamento (UE) 2016/679, deficiencia no subsanada por la Ley Orgánica 3/2018, la cual ni tan siquiera las define.

El delegado de protección de datos es una figura creada por el Reglamento (UE) 2016/679 del Parlamento 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.

El DPO es el profesional, en persona física o jurídica, encargado de informar al responsable o al encargado de sus obligaciones en la materia del Reglamento (EU) 2016/679 y Ley Orgánica 3/2018. Además, el DPO deberá velar por el cumplimiento de estas dos normas en la organización, colaborando con las autoridades de control y siendo a, su vez, el nexo de unión entre de la organización tratante de los datos y la entidad de control correspondiente.

El responsable del tratamiento de datos o el cargado del tratamiento de datos, artículo 37 del Reglamento (UE) 2016/679, publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la Autoridad de control, artículo 37.7 del Reglamento (UE) 2016/679.

La norma de protección de datos determina los supuestos en los que se requiere la presencia de un delegado de protección de datos y también determina la naturaleza de

[333] *Vid Supra p 95,* capítulo 3, del Título I.

[334] LAZPIRA GURTUBAN M. (1994), (1994) "Análisis comparado …..", op.cit; pp 397 y ss.

esta figura dentro de la organización que depende del responsable o encargado del tratamiento[335].

El Reglamento (UE) 2016/679 dedica la sección 4 del Capítulo IV, sobre el responsable del tratamiento y encargado del tratamiento, al DPO. En esta sección se encuentran el artículo 37 sobre designación del delegado de protección de datos, el artículo 38 que trata la posición del delegado de protección de datos, y el artículo 39 sobre las funciones del delegado de protección de datos.

La Ley Orgánica 3/2018, sigue la misma sistemática que el Reglamento (UE). El Capítulo III dedicado al delegado de protección de datos lo incluye dentro del Título V relativo al responsable y encargado del tratamiento. El Capítulo III sobre el delegado de protección de datos contiene el artículo 34 sobre designación de un delegado de protección de datos, el artículo 35 que trata de la cualificación del delegado de protección de datos, el artículo 36 sobre la posición del delegado de protección de datos y el artículo 37 que describe la intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

Los aspectos relevantes y característicos de esta figura, que trataremos en este apartado, son: su independencia, su designación, su revocación, los requisitos para ser designado, las modalidades de contratación, sus funciones, sus obligaciones y su régimen de responsabilidad y, por último, la relación que tiene con el responsable del tratamiento de datos y con el encargado del tratamiento de datos, en su caso.

4.1.1.Independencia

Una de las características que definen al delegado de protección de datos es su independencia en relación a la personas o personas que le nombran, designan o contratan[336].

En este orden de cosas, el artículo 38, posición del delegado de protección de datos, del Reglamento (UE) 2016/679 dedica una serie de epígrafes a esta condición del delegado de protección de datos. El Reglamento (UE) no utiliza el término “independencia” en el caso del delegado de protección de datos, mientras si lo utiliza en otras figuras como son el Comité Europeo de Protección de datos, artículo 69, las autoridades de control, artículo 52, los organismos de certificación, artículo 43, en el artículo 38 introduce una serie de condicione que de hecho garantizan su independencia.

EL artículo 38 sobre Posición del delegado de protección de datos en su apartado 3, advierte al responsable y al encargado del tratamiento que deben garantizar que el

[335] AEPD (2020) “Delegado de protección de datos”. Junio 2020. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/ delegado- de-proteccion-de-datos. (31/01/2021).

[336] AEPD (2019) “Manual del delegado de protección de datos”. Guía para los Delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del. Reglamento General de Protección de Datos de la Unión Europea. Julio de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-12/El%20Manual%20del%20DPD%20-%20KORFFGEORGES%20-%20ESP.pdf (31/01/2021). p 121.

delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones.

Además, el mismo apartado 3 obliga al responsable y al encargado del tratamiento a no sancionar o cesar al delegado de protección de datos por desempeñar sus funciones. Así pues, parece que la voluntad del Reglamento (UE) es la de profundizar en esta independencia del delgado de protección de datos, estipulado que el delegado solo rendirá cuentas al más alto nivel jerárquico del responsable o encargado y lo hará directamente, es decir, sin intermediación.

El apartado 4 del artículo 38 permite y a su vez legitima que el interesado pueda contactar directamente, sin intermediarios, con el delegado de protección de datos cuando desee tratar asuntos relacionados con el tratamiento de sus datos personales o cuando desee ejercer sus derechos al amparo de la legislación de protección de datos.

El secreto al que referencia el apartado 5 del artículo 34 no excluye al responsable o al encargado del tratamiento con lo que refuerza el valor de la independencia que el propio Reglamento (UE) le asigna.

Finalmente, el artículo 34 garantiza que el responsable o encargado que las funciones del delegado de protección de datos cuando confluyan en un profesional con otros desempeños en la misma organización no den lugar a conflicto de intereses, pues contravendría su independencia además de otros preceptos legales.

La Ley Orgánica 3/2018 es más explícita que el Reglamento en cuanto a la independencia del delegado de la protección de datos. El artículo 36, sobre posición del delegado de protección de datos, en su apartado 2 dice: "Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses".

> Como norma general, los cargos en conflicto dentro de una organización pueden incluir los puestos de alta dirección (tales como director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI) pero también otros cargos inferiores en la estructura organizativa si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento. Asimismo, también puede surgir un conflicto de intereses, por ejemplo, si se pide a un DPD que represente al responsable o al encargado del tratamiento ante los tribunales en casos relacionados con la protección de datos[337].

4.1.2. Designación y revocación

La designación tendrá carácter obligatorio o carácter voluntario. Tendrá carácter obligatorio, artículo 37.1 del Reglamento (UE) 2016/679, siempre que el tratamiento lo

[337] COMISIÓN EUROPEA. "Directrices sobre los delegados de protección de datos (DPO)". Adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017. Grupo de trabajo sobre protección de datos del artículo 29. Disponible en https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf (28/02/2021). p 18.

lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.

Este carácter obligatorio del Reglamento (UE) queda perfectamente claro cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala o cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

La Ley Orgánica 3/2018 en su artículo 34.1, sobre designación de un delegado de protección de datos, amplia la lista del Reglamento (UE) sobre las situaciones en las que se debe designar, por el responsable o el encargado, a un DPO. Este listado de obligados es el que se describe a continuación:

a. "Los colegios profesionales y sus consejos generales.
b. Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
c. Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
d. Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
e. Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
f. Los establecimientos financieros de crédito.
g. Las entidades aseguradoras y reaseguradoras.
h. Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
i. Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
j. Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
k. Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
l. Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

   Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m. Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
n. Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
o. Las empresas de seguridad privada.
p. Las federaciones deportivas cuando traten datos de menores de edad."

Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar siempre y en cualquier caso de manera voluntaria a un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica, artículo 34.2 La Ley Orgánica 3/2018.

Así pues, concluyendo, hay dos tipos de designaciones, las obligatorias, a las que está obligado el responsable y el delegado, y las voluntarias, las designaciones realizadas a criterio del responsable y del encargado de tratamiento de datos.

Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño (artículo 37.3 del Reglamento (UE) 2016/679). La Ley Orgánica 3 /2018, no incluye esta habilitación en su articulado, lo cual no impediría que se pudiera utilizar siempre que no contradiga el artículo 34 de la Ley Orgánica 3/2018.

El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39, artículo 37.5 del Reglamento (UE) 2016/679). La ley abunda y amplia el requisito de idoneidad del delegado de protección de datos, introduciendo el mérito de los certificados de capacitación voluntarios, artículo 35 La Ley Orgánica 3/2018.

El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios, artículo 37.6 del Reglamento (UE) 2016/679.

Una vez que el responsable o el encargado del tratamiento, con carácter voluntario y obligatorio, haya nombrado, designado o cesado al delegado de la protección de datos lo comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos[338].

4.1.3.Requisitos

El legislador al crear por primera vez la figura del delegado de protección de datos no ha querido dejar al criterio de los países Miembros la cualificación profesional de dichas personas, físicas o jurídicas. A tal efecto ha introducido en el artículo 37, sobre

[338] AEPD (2020) "Delegado de protección de datos". Junio 2020. Disponible en https://www.aepd.es/es/ derechos-y-deberes/ cumple-tus-deberes/ medidas-de-cumplimiento/delegado-de-proteccion-de-datos (31/01/2021).

designación del delegado de protección de datos, una serie de aspectos relativos a dicha cualificación.

En el caso de España, el legislador, ha mejorado o ha incrementado el nivel de exigencia en cuanto a los requisitos para que una persona física o jurídica pueda ser nombrada o designada delegado de protección de datos.

Reglamento (UE) 2016/679, artículo 37.5, de designación del delegado de protección de datos, dice:

> "El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39."

Reglamento (UE) 2016/679 dedica el epígrafe 5 del artículo 37 para establecer que el delegado de protección de datos deberá estar en posesión de cualidades profesionales para que pueda ser designado como tal. Además, añade que deberá disponer de conocimientos especializados en derecho.

A la cualificación profesional, a sus conocimientos en derecho, el Reglamento (UE) exige que el delegado en protección de datos antes de su nombramiento, contrato o designación debe tener práctica en materia de protección de datos. Es decir, la condición de la experiencia en estas materias sobre datos e información deberá tenerse en cuenta.

A todo ello, el Reglamento (UE) añade que también deberá ser requisito para el nombramiento o designación del delegado de protección de datos la capacidad para desempeñar las funciones indicadas en el artículo 39 de la persona que pretenda ser designada.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, también dedica un artículo a los requisitos para la designación del delegado de protección de datos, en concreto es el artículo 35 el que describe tales extremos.

El artículo 35 de la Ley Orgánica 3/2018 se titula "Cualificación del delegado de protección de datos", lo cual pone de manifiesto la importancia que el legislador español ha dado a tal cuestión a la hora de redactar la ley, lejos de la forma que el Reglamento (UE) trata el mismo tema.

El artículo 35 de la Ley Orgánica 3/2018 se remite al artículo 37.5 del Reglamento (UE) 2016/679, aunque introduce nuevos requisitos.

Los requisitos añadidos por la Ley Orgánica 3/2018 sobre los que ya expone el Reglamento (UE) 2016/679, son:

1. El candidato deberá poder demostrar que cumple los requisitos. La ley dice concretamente: "podrá demostrarse, entre otros medios, a través de", lo cual manifiesta que en el caso de no poderse demostrar no podrá ser tenido en cuenta.

El reglamento no entra estos extremos pues tan solo dice: "será designado atendiendo a".

2. Aparecen los mecanismos de certificación de los requisitos que presenta el candidato como mecanismo voluntario para la demostración de los mismos. El Reglamento (UE) no menciona estos mecanismos.
3. La titulación universitaria que acredite conocimientos especializados en el derecho exigido por la Ley orgánica 3/2018. El Reglamento (UE) tan solo dice: "sus conocimientos especializados del Derecho".
4. La práctica en materia de protección de datos, que ya aparece en el Reglamento (UE).

4.1.4. Modalidades de contratación

En relación con el modo de designación o relación entre el responsable o encargado del tratamiento y el delegado de protección de datos, el Reglamento (UE) se pronuncia de forma explícita mientras que la Ley Orgánica 3/2018 no lo hace de la misma forma.

Las formas o modalidades de contratación entre el responsable o encargado del tratamiento y el delegado de protección de datos son bien el contrato laboral, se entiende en cualquier de sus modalidades, o bien el contrato de prestación de servicios profesionales de los artículos 1.252 al 1.314 del Código Civil[339].

En este orden de cosas, es el artículo 37.6 del Reglamento 2016/679, el que afirma que el delegado de protección de datos podrá forma parte de la plantilla de la organización de trabajo del responsable o del encargado, en consecuencia, se refiere a la modalidad de contrato laboral. Así pues, se entiende que podía ya formar parte de la plantilla antes de su nombramiento y que también puede ser contratado a tal fin.

Por otra parte, el propio artículo 37. 6 permite que el delegado de protección de datos podrá desempeñar sus funciones en el marco de un contrato de servicios. En consecuencia, podrá tratarse de un profesional que actúe conforme al régimen especial de trabajadores autónomos[340] o de una empresa o sociedad que oferte y provea este tipo de servicios.

En el caso de que el servicio lo preste una empresa o sociedad se podrá utilizar el contrato de prestación de servicios de los artículos 1.542 al 1.545 y 1.583 del Código Civil[341].

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales no hace ninguna referencia a lo dictado por el artículo 37.6 del Reglamento (UE), pero en su artículo 34.5 establece que en el cumplimiento de las obligaciones de los responsables y encargados del tratamiento, estos podrán establecer

[339] Código Civil del Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

[340] Ley 18/2007, de 4 de julio, por la que se procede a la integración de los trabajadores por cuenta propia del Régimen Especial Agrario de la Seguridad Social en el Régimen Especial de la Seguridad Social de los Trabajadores por Cuenta Propia o Autónomos.

[341] CÓDIGO CIVIL del Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

que el delegado tenga dedicación completa o dedicación a tiempo parcial, en base al volumen de trabajo que pueda tener el DPO en relación a sus funciones.

4.1.5. Funciones, obligaciones y régimen de responsabilidad

Las funciones del delegado de protección de datos, documento que publica la AEPD en agosto 2019, serán de información, asesoramiento y supervisión, y se encuentran especificadas en el artículo 39 del RGPD y 34 y siguientes de la Ley Orgánica 3/2018, así como en el documento "directrices los delegados de protección de datos" de la AEPD[342].

El delegado de protección de datos tendrá las funciones de supervisar y gestionar. Por una parte, supervisará el cumplimiento de la normativa de protección de datos personales y, por la otra parte, cuando así se lo requiera el interesado gestionará las consultas en relación con el tratamiento de sus datos personales.

El Reglamento (UE) 2016/679 en su artículo 37.6 dice que: "el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado de tratamiento o desempeñar sus funciones en el marco de un contrato de servicios". Se desprende del conjunto del Reglamento (UE) 2016/679 y la Ley Orgánica, además, que quedan excluidos los que tengan conflictos de intereses tales como pueden ser los de RRHH, Informática y Gestión Económica, en base a los artículos en prevención del conflicto de intereses del delegado, Reglamento (UE) artículo 38.6 y Ley Orgánica 3/2018 artículo 36.2.

Por otra parte, del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 se concluye que el delegado de protección de datos debe desempeñar sus funciones dentro de las dependencias del centro responsable, es decir, en sus instalaciones.

De la lectura del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, se desprende, tal como ya se ha comentado en varias ocasiones, que el delegado de protección de datos depende del responsable o encargado del tratamiento, sin que esté sometido a las instrucciones de ningún estamento de la organización o compañía, por las condiciones del art. 38 RGDP, puntos 3 y 5.

En cuanto a la relación del delegado de protección de datos con el Comité de Protección de Seguridad de Datos, en base a lo que indica el art. 38 del RGDP, este no podría ser miembro de dicho Comité y en el caso de que el Comité requiera su presencia los hará como invitado con voz, pero sin derecho a voto. Además, tal como se verá más adelante uno no sustituye al otro[343].

Las funciones del delegado de protección de datos (artículo 39 RGDP) son el asesoramiento general en todo lo relativo a la protección de datos personales y de las obligaciones que impone el Reglamento (UE) 2016/679 y de otras obligaciones de otras

[342] Grupo de trabajo sobre protección de datos del artículo 29. Adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017. Creado en virtud del artículo 29 de la Directiva 95/46/CE. Órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de la Directiva 5/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

[343] *Vid Infra p 414,* capítulo 6.1.2, del Título III.

disposiciones de protección de datos de la Unión o de los Estados miembros. Aunque, concretamente deberá cumplir:

1. Supervisión y auditorías:
    a. del cumplimiento del Reglamento (UE) 2016/679 y de otra legislación de protección de datos de aplicación,
    b. de las políticas en materia de protección de datos (de privacidad),
    c. de la asignación de responsabilidades, la concienciación y formación del personal implicados y obligados por la normativa,
2. La elaboración de informes de evaluación de impacto de ciertos tratamientos de datos personales del artículo 35 del RGDP.
3. La cooperación con la autoridad de contro.l
4. Actuar como punto de contacto de la Autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar, consultas, en su caso, sobre cualquier otro asunto.

Las funciones del delegado de protección de datos le obligan a realizar las siguientes siete tareas, de la lectura del Reglamento (UE) 2016/679 se desprende:

A) Auditoría:
    - de protección de datos,
    - realización de evaluaciones de impacto sobre la protección de datos,
    - análisis de riesgo de los tratamientos realizados.
B) Relaciones con las autoridades de supervisión.
C) Diseño e implantación de:
    - políticas de protección de datos,
    - de medidas de información a los afectados por los tratamientos de datos,
    - de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuados a los riesgos y naturaleza de los tratamientos,
    - de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos,
    - de programas de formación y sensibilización del personal en materia de protección de datos,
    - del cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
D) Valoración:
    - de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos,
    - de las solicitudes de ejercicio de derechos por parte de los interesados.
E) Establecimiento de:
    - mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados,

- la gestión de los registros de actividades de tratamiento,
- procedimientos de gestión de violaciones de seguridad de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados,
- la necesidad de realización de evaluaciones de impacto sobre la protección de datos,
- la identificación de las bases jurídicas de los tratamientos.

F) Identificación de:

- los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- la existencia de normativa sectorial que pueda determinar condiciones de tratamiento especificas distintas de las establecidas por la normativa general de protección de datos. proteger los derechos que protege o reduce el impacto de lo que el Reglamento protege y que consta en su artículo 1, artículo 1 sobre el Objeto del Reglamento (UE) 2016/679, y en el ámbito de su artículo 2, sobre el Ámbito de aplicación material del Reglamento (UE) 2016/679, y el artículo 3, sobre el Ámbito territorial del Reglamento (UE) 2016/679.

G) Gestión de reclamaciones:

- Gestión de reclamaciones. Actuará o podrá actuar como instancia previa a una reclamación frente a la Agencia Española de Protección de Datos, cuando así el afectado lo desee, debiendo comunicar la decisión al afectado en el plazo máximo de dos meses, artículo 37 de la Ley Orgánica 3/29018.

4.2. Relación con el responsable de tratamiento y con el encargado de tratamiento

El Reglamento (UE) 2016/679 define la figura del responsable del tratamiento en su artículo 4, definiciones. El punto 7) del citado artículo dice que el responsable del tratamiento o responsable es:

> "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

El Reglamento (UE) 2016/679 define la figura del encargado del tratamiento en su artículo 4, definiciones. El punto 8) encargado del tratamiento o encargado dice: "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento."

En este orden de cosas, en el mencionado artículo 4 no aparece la definición de delegado de protección de datos. Por otra parte, el Reglamento (UE) 2016/679 dedica un artículo, artículo 28, a describir actividades del encargado del tratamiento, pero no dedica ningún artículo al responsable del tratamiento como tal, la situación no es subsanada por la Ley

Orgánica 3/2018. Sin embargo, también es cierto que el Reglamento (UE) 2016/679 dedica el artículo 24 a la responsabilidad del responsable del tratamiento.

El Reglamento (UE) 2016/679, en su capítulo IV, sobre el responsable del tratamiento y encargado del tratamiento, introduce la figura del DPO, en su Sección 4, en los artículos 37, 38 y 39. Si embargo, como ya se ha reseñado con anterioridad, ninguno de estos tres artículos define la figura de DPO, si bien la vincula jerárquicamente al responsable o al encargado del tratamiento, cuando en su artículo 37.1. reza: "El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que".

Tal como ya se ha comentado anteriormente, el Reglamento (UE) 2016/679 define, insuficientemente, al responsable y al encargado del tratamiento. Esta insuficiencia no es subsanada por la Ley Orgánica 3/2018, que ni tan siquiera entra en la definición ni de una ni de la otra figura, pero dedicando el artículo 33 al "encargado del tratamiento".

El contenido del artículo que trata de la designación del DPO en el Reglamento (UE) 2016/679 es ampliado por la Ley Orgánica 3/2018 en su artículo 34.1, sobre designación de un delegado de protección de datos, en el cual estipula que los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679.

La relación entre el DPO y el responsable o encargado del tratamiento no tan solo se limita a su nombramiento, designación o contratación, sino que también existe en cuanto a la obligación del responsable de ofrecer y dar los datos del delegado de protección de datos a las personas que suministren sus datos a los responsables del tratamiento, artículo 13 del Reglamento (UE) 2016/679. También facilitará los datos del delegado de protección de datos cuando los datos personales no se hayan obtenido del interesado, artículo 14 del Reglamento (UE) 2016/679.

En las situaciones en las que el responsable del tratamiento esté obligado por el Reglamento (UE) a realizar una evaluación del impacto relativa a protección de datos y este responsable haya designado a un DPO, este contará con el criterio del delegado de protección de datos al realizar la evaluación, artículo 35 del Reglamento (UE) 2016/679.

El responsable del tratamiento cuando realice una consulta previa a la Autoridad de control, una vez haya sospechas fundadas de que el tratamiento presenta un alto riesgo de lesionar los derechos de las personas en materia de protección como consecuencia de la evaluación de impacto realizada, facilitará los datos del DPO, artículo 36 del Reglamento (UE) 2016/679.

La relación del responsable o el encargo del tratamiento de datos con el DPO será de vinculación contractual pero no de subordinación funcional, de tal forma que el delegado de protección de datos gozará de la suficiente independencia de criterio y de acción respecto de sus funciones, artículo 38.3 del Reglamento (UE) 2016/679), así como estará dotado de todos los recursos necesarios para el desempeño de sus funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el

mantenimiento de sus conocimientos especializados, artículo 38.2 del Reglamento (UE) 2016/679.

4.3. Intervención del delegado de protección de datos en caso de reclamación, Ley Orgánica 3/2018

La Ley Orgánica 3/2018 incorpora en España una nueva función al delegado de protección de datos, esta nueva función viene estipulada en el artículo 37 sobre la "Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos"[344]. También la de intervención del DPO surge cuando el afectado presenta una reclamación ante la autoridad de control y esta remite esta reclamación al DPD de la entidad dándole un plazo de respuesta de un mes, artículo 65.4 de la Ley Orgánica 3/2018.

El derecho a presentar una reclamación ante una autoridad de control está reconocido por el Reglamento (UE) 2016/679 en sus artículos 13, 14, 15, 47, 77, sobre derecho a presentar una reclamación ante una autoridad de control, y 79.

La Ley Orgánica 3/2018 dedica el Título VIII a los procedimientos en caso de posible vulneración de la normativa de protección de datos, es decir, a la tramitación de una reclamación.

La Ley Orgánica 3/2018, le da al delegado de protección de datos un papel fundamental en la resolución de reclamaciones.

En este orden de cosas, la persona interesada en presentar una reclamación por incumplimiento del RGPD puede dirigirse directamente al DPO de la entidad contra la que se reclame, antes de presentar la reclamación ante la Agencia Española de Protección de Datos o autoridad autonómica de protección de datos.

En el caso de que la persona afectada presentará una reclamación ante el DPO este dispondrá de un plazo máximo de dos meses, desde su recepción, para notificar su decisión.

En este supuesto el DPO dispone de un mes para notificar su decisión a la Autoridad de control. En el supuesto de que el DPO no notificara respuesta a la Autoridad de control, se prosiguiera según lo establecido en el Título VIII de la Ley Orgánica 3/2018.

[344] BOTELLA PAMIES, E. (2019) "Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos" en Arenas Ramiro, M. (dir.), Ortega Giménez, A.(dir.), "Protección de datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)". Editorial Sepin. pp 198-200.

Capítulo 5. La autorregulación en la protección de datos

5.1. Los códigos de conducta

En los textos legales de protección de datos en 1992 y 1999, los códigos de conducta, llamados códigos tipo, se entendían como códigos deontológicos o de buena práctica profesional, artículo 31 de la Ley Orgánica 5/1992 y artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre.

Con carácter general, por código de conducta se suele entender un documento sobre ciertos principios, valores o procedimientos, suscrito voluntariamente por una organización y que se compromete a cumplir unilateralmente. Es muy habitual que los colegios profesionales editen sus códigos deontológicos, normas autoproclamadas en donde se reflejan los valores deontológicos y/o profesionales que se exigen al profesional perteneciente a la institución.

En el ordenamiento jurídico español aparece la expresión Código de Conducta en Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. El Capítulo VI de este texto normativos se dedica es relativo a "Deberes de los empleados públicos. Código de Conducta". Para explicar el Código de Conducta el artículo 52 del en Real Decreto Legislativo 5/2015, dice:

> "Los empleados públicos deberán desempeñar con diligencia las tareas que tengan asignadas y velar por los intereses generales con sujeción y observancia de la Constitución y del resto del ordenamiento jurídico, y deberán actuar con arreglo a los siguientes principios: objetividad, integridad, neutralidad, responsabilidad, imparcialidad, confidencialidad, dedicación al servicio público, transparencia, ejemplaridad, austeridad, accesibilidad, eficacia, honradez, promoción del entorno cultural y medioambiental, y respeto a la igualdad entre mujeres y hombres, que inspiran el Código de Conducta de los empleados públicos configurado por los principios éticos y de conducta regulados en los artículos siguientes".

En el contexto de la protección de datos, la expresión de Códigos de Conducta, parece por primera vez en el artículo 27 del Capítulo V, sobre códigos de conducta, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Para esta norma los códigos de conducta estaban destinados a contribuir a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva, en base a las peculiaridades de cada organización, y tenían naturaleza voluntaria.

Los Códigos de Conducta, en el Reglamento (UE) 2016/679, aparecen en el artículo 40, de códigos de conducta, Sección 5, sobre códigos de conducta y certificación, del Capítulo IV, sobre el responsable del tratamiento y encargado del tratamiento.

A efectos del Reglamento (EU) 2016/679, los Códigos de Conducta podrán ser elaborados por asociaciones y otros organismos representativos de categorías de

responsables o encargados del tratamiento, o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, artículo 40.2 del Reglamento (UE) 2016/679.

El Reglamento (UE) menciona que la adhesión a un Código de Conducta permitirá al responsable, artículo 32.3 del Reglamento (UE) 2016/679, y al encargado, artículo 28.5 del Reglamento (UE) 2016/679, del tratamiento demostrar la existencia de garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado, artículo 28.5 del Reglamento (UE) 2016/679. Sin embargo, tal como se explica en la Nota Crítica, en el final de este apartado, desde un punto de vista práctico y en base a la lógica de los hechos, la adhesión a un código de conducta lo único que demuestra es la intención de quien se adhiere, pero no su cumplimiento.

El antecedente de la expresión del código de conducta en España se encuentra en los "Códigos Tipo" del artículo 32, sobre códigos tipo, Capítulo II, de ficheros de titularidad privada, Titulo IV, sobre disposiciones sectoriales, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Este artículo 32 es prácticamente el mismo que el artículo 31 y que aparece, por primera vez, en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter.

La Ley Orgánica 3 /2018 sitúa a los códigos de conducta en el artículo 38, en el Capítulo IV, sobre códigos de conducta y certificación, del Título V, de los responsable y encargado del tratamiento, y serán vinculantes para quienes se adhieran a los mismos. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

Los proyectos de código serán sometidos al mecanismo de coherencia, artículo 63 de Reglamento (UE) 2016/679, a través de la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos en los supuestos en que ello proceda según su artículo 40.7, artículo 40.7 del Reglamento (UE) 2016/679[345]. El procedimiento quedará suspendido en tanto el Comité Europeo de Protección de Datos no emita el dictamen.

Cuando una autoridad autonómica de protección de datos someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta Ley Orgánica, artículo 60 de la Ley Orgánica 3/2018.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado

[345] AEPD (2020) Sede electrónica de 27 de noviembre de 2020. "Códigos de Conducta". Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta (28/02/2021).

por el Comité Europeo de Protección de Datos, artículo 40.11 del (UE) 2016/679. El registro será accesible a través de medios electrónicos.

Por último, hay que añadir que la Norma Internacional ISO 9001, sobre sistemas de gestión de la calidad, en su página 25, en el Anexo B sobre Otras Normas Internacionales sobre gestión de la calidad y sistemas de gestión de la calidad desarrolladas por el Comité Técnico ISO/TC 176 y en relación a los códigos de conducta, establece que la ISO 10001 Gestión de la Calidad — Satisfacción del cliente — Directrices para los códigos de conducta de las organizaciones, proporciona orientación a una organización para determinar que sus disposiciones para lograr la satisfacción del cliente cumplen las necesidades y expectativas del cliente. Su uso puede aumentar la confianza del cliente en una organización y mejorar la comprensión del cliente sobre lo que espera de una organización, reduciendo por lo tanto la probabilidad de malentendidos y quejas. [346]

Nota crítica: El Reglamento (UE) menciona que la adhesión a un código de conducta permitirá al responsable y al encargado del tratamiento demostrar la existencia de garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

Sin embargo, esta aseveración es sorprendente. Desde un punto de vista práctico y en base a la lógica de los hechos, la adhesión a un código de conducta lo único que demuestra es la intención de quien se adhiere, pero no su cumplimiento.

Este error del Reglamento (UE) o esta expresión tendente a producir confusión es subsanada por la Ley Orgánica 3/2018. Esta Ley en su artículo 38, sobre códigos de conducta, entiende que el responsable del tratamiento podrá someter la verificación de la conformidad de este con las materias sujetas al código de conducta.

La adhesión a un código de conducta o la elaboración de un código de conducta no garantiza su cumplimiento, sino que debe ser una auditoría externa e independiente la que deberá valorar y certificar, en su caso, dicho cumplimiento.

5.2. Certificación. Sello Europeo de Protección de Datos

La certificación es un procedimiento de verificación, llevado a cabo por un organismo independiente y autorizado, del cumplimiento por parte de una organización de un estándar que debe cumplir, bien por imperativo normativo o bien por propia decisión.

Habitualmente la certificación es elaborada por una red de expertos, dentro de un sistema basado en la confianza y en el intercambio de conocimientos y de experiencias. En general cualquier actividad que tenga por objeto evaluar si un producto, servicio, sistema, instalación, etc. es conforme con ciertos requisitos puede estar sujeta a acreditación[347].

[346] MARCOS, T. (2018) "Renovando la satisfacción del cliente". Revista de la normalización española, 2. Disponible en https://revista.une.org/ 2/renovando-la-satisfaccion-del-cliente.html. (31/05/2021).

[347] ENAC (2020) Entidad Nacional de Acreditación. "¿Qué es la acreditación?". Disponible en https://www.enac.es/web/enac/que-hacemos/-que-es-la-acreditacion- (31/01/2021).

La certificación es tratada por el Reglamento (UE) en el artículo 42 con carácter voluntario[348]. A fin de aumentar la transparencia y el cumplimiento del Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes, Considerando 100 del Reglamento (UE) 2016/679.

La certificación que trae el Reglamento (UE) reúne las siguientes características, artículo 42 del Reglamento (UE) 2016/679:

1. Voluntariedad. La solicitud de un certificado será siempre voluntaria.
2. Transparencia. Estará disponible a través de un proceso transparente.
3. Responsabilidad. No limitará la responsabilidad del responsable o encargado del tratamiento.
4. Expedición. Será expedida por los organismos de certificación. Estos organismos son los que se refiere el artículo 43 o por la Autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité, de conformidad con el artículo 63.
5. Sello Europeo de Protección de Datos. Cuando los criterios sean aprobados por el Comité, artículo 42.5 del Reglamento (UE) 2016/679, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.
6. Información completa. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación darán al organismo de certificación mencionado en el artículo 43, o en su caso a la Autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.
7. Tiempo de duración. Tres años. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años.
8. Renovación. Podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes.
9. Retirada de la certificación. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la Autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.
10. Registro del Comité Europeo de Protección de Datos. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

En la Ley Orgánica 3 /2018 la certificación y las instituciones de certificación vienen estipuladas por el artículo 39, sobre acreditación de instituciones de certificación, del

[348] PRIETO HERGUERA, J (29 junio 2016) "Códigos de Conducta, certificaciones y trasferencias internacionales" 8.ª Sesión Anual Abierta de la AEPD. Gran Auditorio Ramón y Cajal.

Capítulo IV, de códigos de conducta y certificación, del Título V, responsable y encargado del tratamiento.

Sin perjuicio de las funciones y poderes de acreditación de la Autoridad de control competente, artículos 57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación, artículo 43.1 del Reglamento (UE) 2016/679, podrá ser llevada a cabo por la Entidad Nacional de Acreditación[349], que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las Comunidades Autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

5.3. Organismos de certificación

Los organismos de certificación aparecen regulados en el artículo 43, de organismo de certificación, de la Sección 5, códigos de conducta y certificación, del Reglamento (UE) 2016/679. En tal sentido, dicho artículo estipula que, sin perjuicio de las funciones y poderes de la Autoridad de control competente, artículos 57 y 58 del Reglamento (UE) 2016/679, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informadas las autoridades de control, a fin de estas que puedas ejercer, si así se requiere, artículo 58.2.h) Reglamento (UE) 2016/679.

Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos, en base a los criterios expuesto en el artículo 43.2 del Reglamento (UE) y que se harán públicos, artículo 43.6 Reglamento (UE) 2016/679.

Estos organismos que podrán acreditar a los certificadores son por una parte la Autoridad de control que sea competente, artículos 55 y 56 Reglamento (UE) 2016/679) y por la otra, el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.o 765/2008 del Parlamento Europeo y del Consejo con arreglo a la norma EN-ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la Autoridad de control que sea competente, artículos 43, 55, 56 del Reglamento (UE) 2016/679.

La acreditación emitida por la Autoridad de control o por el organismo nacional de acreditación tendrá una vigencia o validez máximo de cinco años. Esta acreditación podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el artículo 43 del Reglamento (UE).

[349] Ley 21/1992, de 16 de julio, de Industria; el Real Decreto 1715/2010, de 17de diciembre; Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008.

Capítulo 6. Los mecanismos de cooperación y coherencia presentes en la normativa de protección de datos

6.1. El mecanismo de coherencia

Los mecanismos de coherencia vienen reflejados en el artículo 63, sobre mecanismos de coherencia, de la sección 2, de coherencia, del Reglamento (UE) 2016/679. El mecanismo de coherencia es un marco en el cual se arbitran medidas y procedimientos que se establecen entre las autoridades de control y la Comisión Europea, en base al Reglamento (UE) 2016/679 y en torno al Comité Europeo de Protección de datos, artículo 63 del Reglamento (UE) 2016/679.[350]

En este orden de cosas, se establece un primer mecanismo en el momento que una autoridad de control trate alguna de las medidas que se enumeran a continuación, frente a lo cual el Comité Europeo de Protección de Datos emitirá un dictamen. Los temas que activan este dictamen son, artículo 64 del Reglamento (UE) 2016/679:

a) Disponer de una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto, artículo 35 del Reglamento (UE) 2016/679, relativa a la protección de datos.
b) Disponer que un código de conducta, artículo 40 del Reglamento (UE) 2016/679, o una modificación o ampliación de un código de conducta es conforme con el Reglamento (UE) 2016/679.
c) Aprobar los criterios aplicables a la acreditación de un organismo que supervise los códigos de conducta.
d) Aprobar los criterios aplicables a la acreditación de un organismo de certificación, artículo 43 del Reglamento (UE) 2016/679.
e) Aprobar de normas corporativas vinculantes, artículo 47 del Reglamento (UE) 2016/679
f) Determinar las cláusulas tipo de protección de datos.
g) Autorizar las cláusulas contractuales. El Reglamento habla de cláusulas contractuales: cuando se refiere a los contratos entre responsable y encargado del tratamiento.

A estas siete cuestiones que activan al Comité para emitir un dictamen, hay que añadir que el Comité emitirá una orden ejecutiva o un dictamen para las "decisiones de adecuación" de protección de datos, artículo 45 del Reglamento (UE) 2016/679[351].

Cualquier Autoridad de control y el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua o las operaciones conjuntas.

[350] GARCIA GONZALO, R. (2 julio 2028) "Mecanismos de Coherencia". AEPD-UIMP, Santander 2 de julio de 2018.
[351] *Vid Supra p 185* capítulo 1.2.1. Título II.

El dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Este plazo tendrá efectos suspensivos a efectos de la decisión de la Autoridad de control competente.

El Comité Europeo de Protección de Datos emitirá dictamen siempre que no haya emitido ya un dictamen sobre el mismo asunto, es decir, si ya se emitió un dictamen sobre una cuestión determinada el Comité no emitirá un segundo dictamen sobre la misma cuestión.

Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité Europeo de Protección de Datos, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas. La Presidencia del Comité Europeo de Protección de Datos lo informará, y publicará, sin dilación indebida por medios electrónicos, a:

- a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, las traducciones de la información que sea pertinente,
- a la Autoridad de control competente,
- a la Comisión del dictamen.

Cuando la Autoridad de control interesada informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará lo previsto para la resolución de conflictos, artículo 65.1 del Reglamento (UE) 2016/679.

Dentro del mecanismo de coherencia se encuentra, por un parte, la norma corporativa vinculante cuando falta una decisión de adecuación emitida por el Comité Europeo de Protección de Datos y, por otra parte, las cláusulas tipo a falta de decisión de adecuación y de norma corporativa vinculante. Ambas se desarrollan en los dos siguientes apartados.

6.1.1.Normas corporativas vinculantes

La norma corporativa vinculante es un instrumento que el Reglamento pone a disposición de la Autoridad de control de cada país miembro.

La norma corporativa vinculante se incluye como uno de los parámetros que activan al Comité Europeo de Protección de Datos, dentro de los mecanismos de coherencia del Reglamento y a falta de "decisión de adecuación" del nivel de protección emitida por el Comité Europeo de Protección de Datos, artículo 46.1 del Reglamento (UE) 2016/679[352].

[352] "La Comisión puede reconocer que un tercer país ya no garantiza un nivel de protección de datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes, y a las excepciones aplicadas a situaciones específicas. En ese caso, debe establecerse la celebración de consultas

Las normas corporativas vinculantes son un mecanismo de coherencia relativas a la Transferencias de datos personales a terceros países u organizaciones internacionales del Capítulo V del Reglamento (UE) 2016/679 cuando el Comité no ha emitido una decisión de adecuación relativa al receptor de los datos.

Las normas corporativas vinculantes (o BCR por sus siglas en inglés) son:

> "las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta"[353].

Las normas corporativas vinculantes se entienden y son calificadas por el Reglamento (UE) como "garantías adecuadas" y se aplica este concepto en las transferencias de datos a terceros países u organización internacional, artículo 46.2 del Reglamento (UE) 2016/679.

Las normas corporativas vinculantes contendrán, como mínimo, los siguientes elementos, artículo 47 del Reglamento (UE) 2016/679:

a. "la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros,
b. las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión,
c. su carácter jurídicamente vinculante, tanto a nivel interno como externo,
d. la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes,
e. los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles, el derecho a presentar una reclamación ante la Autoridad de control competente y ante los tribunales competentes de los Estados miembros, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes,
f. la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las

entre la Comisión y esos terceros países u organizaciones internacionales. La Comisión debe informar en tiempo oportuno al tercer país u organización internacional de las razones y entablar consultas a fin de subsanar la situación". STJUE de 16 de julio de 2020 (Gran sala) (asunto C-311/18), apartado 107, p 6.

[353] AEPD (2021) "Transferencias internacionales". Enero 2021. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/ transferencias-internacionales (31/01/2021).

normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro,

g. la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes,
h. las funciones de todo delegado de protección de datos o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones,
i. los procedimientos de reclamación,
j. los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a los interesados,
k. los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la Autoridad de control,
l. el mecanismo de cooperación con la Autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la Autoridad de control los resultados de las verificaciones de las medidas,
m. los mecanismos para informar a la Autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes,
n. la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales."

6.1.1. Cláusulas tipo

La definición de cláusula tipo no viene establecida ni en el Reglamento (UE) 2016/679 ni en la Ley Orgánica 3/2018. Al efecto de conocer su significado jurídico se atiende a la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación, que tiene por objeto la transposición de la Directiva 93/13/CEE, del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores.

La ley 7/1998, en su exposición de motivos, dice: "una cláusula es condición general cuando está predispuesta e incorporada a una pluralidad de contratos exclusivamente por una de las partes, y no tiene por qué ser abusiva".

Las cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes, con independencia de la autoría material de las mismas, de su apariencia externa, de su extensión y de cualesquiera otras circunstancias, habiendo sido

redactadas con la finalidad de ser incorporadas a una pluralidad de contratos, son condiciones generales de la contratación, artículo 1 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación. Aquellas cláusulas contractuales que no hayan sido objeto de negociación individual[354], se pueden entender como cláusulas tipo.

En este orden de cosas, se puede entender que la expresión las "cláusulas tipo", "cláusulas contractuales tipo" o "cláusulas tipo de protección de datos", son condiciones generales de contratación.

Las cláusulas tipo, cláusulas contractuales tipo o cláusulas tipo de protección de datos, en el contexto del Reglamento (UE) 2016/679, se encuentran dentro de los mecanismos de coherencia y son garantías adecuadas para la transferencia de datos a nivel internacional fuera de la Unión Europea a falta de "decisiones de adecuación" y de "normas corporativas vinculantes".

Las cláusulas tipo podrán ser adoptadas por la Comisión Europea, artículo 28.7 del Reglamento (UE) 2016/679, o por las autoridades de control y por la Comisión, artículo 46.2.d) del Reglamento (UE) 2016/679, o por las autoridades de control y sometidas al dictamen del Comité Europeo de Protección de Datos, artículo 28.8 del Reglamento (UE) 2016/679.

A fecha de 12 de junio de 2019, la cláusula tipo de protección de datos adoptadas por la Comisión que siguen siendo válidas [355]:

I. Decisión 2001/497/CE, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales entre responsables del tratamiento a un tercer país y
II. Decisión 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países
III. Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

6.2. Mecanismo de cooperación

El Reglamento (UE) 2016/679 hace referencia a la cooperación en los siguientes casos:

- Cooperación con la Autoridad de control, artículo 31.

[354] Considerando doce de la Directiva 93/13/CEE, del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores.

[355] AEPD (2021) "Transferencias internacionales". Enero 2021. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales (31/01/2021).

- Cooperación internacional en el ámbito de la protección de datos personales, artículo 20.
- Cooperación entre la Autoridad de control principal y las demás autoridades de control interesadas, artículo 60, Sección 1. Capitulo VII.

En este apartado nos dedicaremos a la cooperación entre la Autoridad de control principal y las demás autoridades de control interesadas, dentro de la Sección 1 sobre Cooperación y Coherencia, dentro del Capítulo VII sobre Cooperación y Coherencia.

El objetivo del Reglamento (UE) es que la Autoridad de control principal cooperará con las demás autoridades de control interesadas, dentro del consenso e intercambiando toda información pertinente.

Aunque, también entiende que la Autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua y podrá llevar a cabo operaciones conjuntas en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.

La Autoridad de control principal actuará sin dilación cuando estén en juego los intereses o las funciones de otras autoridades de control.

6.3. Asistencia mutua

El Considerando 133 del Reglamento (UE) 2016/679, entiende que las autoridades de control se deben ayudar una a otra en el desempeño de sus funciones y prestar asistencia mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior.

La asistencia mutua se debe entender como un mecanismo de cooperación cualificado, es decir, materializa una forma activa de cooperación y establece los mecanismos cuando esta se quiebre. Es un mecanismo de cooperación a demanda.

Las autoridades de control se facilitarán, gratuitamente, artículo 61.7 del Reglamento (UE) 2016/679, información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones, artículo 61.1 del Reglamento (UE) 2016/679.

Se podrá negar la asistencia mutua si no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o si el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la Autoridad de control a la que se dirigió la solicitud, artículo 61.4 del Reglamento (UE) 2016/679.

Cuando una autoridad de control no facilite la información, en el plazo de un mes a partir de la recepción de la solicitud de otra Autoridad de control, la Autoridad de control requirente podrá adoptar las medidas que estime oportunas reconocidas en el Reglamento (UE) 2016/679 artículo 55, apartado 1, que le dirigen al artículo 66 apartado 1 y este al artículo 66, apartado 2, que le autoriza a solicitar un Dictamen del Comité Europeo de Protección de Datos, con carácter urgente.

TÍTULO III. RÉGIMEN DE PROTECCIÓN DE DATOS RELATIVOS A LA SALUD Y EN EL AMBITO SANITARIO

Capítulo 1. Concepto jurídico de los datos relacionados con la salud

1.1. Los datos de relativos a la salud dentro del artículo 9 del Reglamento (UE) 2016/679, de Tratamiento de categorías especiales de datos personales

La importancia del dato y su tratamiento para hacer respetar los derechos de las personas en relación a su intimidad y privacidad ha sido reconocida por la Constitución Española en su artículo 18, manifestado por el Tribunal Constitucional en su Sentencia de 4 de mayo[356], y reforzado por el propio Tribunal Constitucional en su Sentencia de 30 de noviembre[357], al definirlo como un derecho autónomo e independiente consistente en el poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Los datos relativos a la salud, su regulación y protección está presente en el ordenamiento jurídico español en varios de sus preceptos, sin ir más lejos la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley 14/2007, de 3 de julio, de Investigación biomédica, entre otros textos legales.

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Así, se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente.

La preocupación internacional por la protección del dato personal ha venido incrementándose a la par que una sociedad cada vez más globalizada. La trascendencia de esta situación se refleja por ejemplo en caso Google Spain S.L. en 2014. El Tribunal de Justicia de la Unión Europea (TJUE) dictó el 13 de mayo de 2014 sentencia[358] sobre el Caso Google vs. España, cuyo objeto eran las cuestiones prejudiciales planteadas por la Audiencia Nacional en el procedimiento entre las demandantes Google Spain, S.L. y Google Inc. y las partes demandas, la Agencia Española de Protección de Datos y un ciudadano español[359].

[356] STC 94/1998 de 4 de mayo (Sala segunda), FJ 4º.

[357] STC 292/2000 de 30 de noviembre (El Pleno), FJ 5º.

[358] STJUE de 13 de mayo de 2014 (Gran sala) (asunto C-131/12), apartado 20, p 7.

[359] LEGALTODAY por y para abogados (17 junio 2014) "Caso Google vs. España: los ciudadanos ante el "derecho al olvido"". Disponible en http://www.legaltoday.com/practica-juridica/civil/nuevas tecnologias/ caso-google-vs-espana-los-ciudadanos-ante-el-derecho-al-olvido (28/02/2021).

Otro caso importante fue el de los datos de Facebook que surgió en 2018, con titulares de prensa como "Facebook reconoce la filtración de datos de más de 120 millones de usuarios" [360] y su repercusión legal con sanción de La Comisión Federal de Comercio de Estados Unidos en julio de 2019 lo cual fue reflejo del titular de prensa "EE. UU. multa a Facebook con 5.000 millones por violar la privacidad de los usuarios"[361].

Las organizaciones europeas se han hecho eco de estas situaciones de riesgo y en este contexto la Comisión público el 4 de noviembre de 2010 una Comunicación "Un enfoque global de la protección de los datos personales en la Unión Europea", embrión de la posterior reforma legislativa en materia de protección de datos de la Unión Europea. A lo cual hay que añadir la jurisprudencia del Tribunal de Justicia de la Unión durante los últimos años, básica para la interpretación de la Comunicación mencionada.

Reflejo de lo comentado es la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes.

El difícil pero a la vez necesario equilibro entre el desempeño de las profesiones dedicadas al cuidado de la salud y en especial médicos, enfermeros, odontólogos y farmacéuticos, entre otros, y los derechos fundamentales de las personas relacionados con su intimidad, privacidad y control de sus propios datos, conlleva a que la regulación de los límites de la legitimidad del tratamiento de los datos personales relativos a la salud de las personas hagan siempre salvedades a situaciones de necesidad vital, salud pública y control de enfermedades transmisibles.

El dato relativo a la salud en el Reglamento (UE) 2016/679 se regula a través de su tratamiento, así pues, el tratamiento del dato personal relacionado con la salud de las personas está prohibido por el artículo 9 del Reglamento (UE) 2016/679, pero esta prohibición está regulada por el apartado 2 en sus puntos h) e i) y por el punto j) al referirse a la actividad de investigación científica, que incluye la de las ciencias de la salud.

De tal forma, el punto 2 del artículo 9 del RGPD dice que esta prohibición no tendrá efectos en determinadas circunstancias y en especial cuando el afectado o la persona interesada de su consentimiento. Sin embargo, este consentimiento no tiene carácter absoluto, dado que el consentimiento no legitimará la excepción de la prohibición cuando las leyes no autoricen tal consentimiento y que concretamente en el caso de la

[360] EL MUNDO (30 junio 2018) "Facebook reconoce la filtración de datos de más de 120 millones de usuario ". Disponible en https://www.elmundo.es/tecnologia/2018/06/30/5b35f2f4468aeb22438b457 d.html (31/05/2020).

[361] Pozzi, S. (12 julio 2019) "EE UU multa a Facebook con 5.000 millones por violar la privacidad de los usuarios". El País. Disponible en https://elpais.com/economia/2019/07/12/ actualidad /1562962870_283549.html (31/05/2020).

salud, aunque esta limitación al consentimiento deberá estar prevista en el Derecho comunitario o en el ordenamiento jurídico español. De alguna forma los aspectos relativos con la salud están muy condicionados por la asimetría de la información[362] entre persona/paciente y profesional de la salud[363] y esta característica también favorece la especial tutela que por parte del derecho se somete a las cuestiones relativas a la salud y en consecuencia la implicación gubernamental[364].

El punto h) del artículo 9 del Reglamento (UE) 2016/679 viene a decir que el consentimiento del interesado no hará falta para tratar los datos de la persona afectada y en consecuencia, no habrá prohibición para el tratamiento de datos, cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3.

Las garantías y condiciones a las que se hacen referencia en el párrafo anterior son, por una parte, que el tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, por otra parte, que el tratamiento sea realizado por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

El punto i) del artículo 9 del Reglamento (UE) 2016/679 informa que el consentimiento del interesado no hará falta para tratar los datos de la persona afectada cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

La base jurídica del secreto profesional como legitimación es analizada con una nota crítica en el capítulo 5.5.3. del Título I.

Resumiendo, las excepciones son las que se aplican en el derecho, excepciones por causa de necesidad o cuando el bien jurídico a proteger es superior al desprotegido

[362] For laying the foundations for the theory of markets with asymmetric information, Teoría sobre la Información Asimétrica de los mercados, le valió a Joseph Eugene Stiglitz (nacido en 1943 en EEUU) compartir el Premio Nobel de Economía en 2001 con George A. Akerlof y Michael Spence.

[363] SPENCE MICHAEL A., ZECKHAUSER R. (1971) "Seguro, Información y Acción Individual". American Economic Review 61 (2), 380-387. Dispone es file:///E:/SPENCE%209PG.pdf. (30/04/2021). p 386.

[364] HIDALGO VELA, A. CORUGEDO DE LAS CUEVAS, I, DEL LLANO SEÑARIAS, J. (2000) “Economía de la salud”. Madrid. Ediciones Pirámide. p 32.

mediante la aplicación de la excepción, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 vienen a concretar los supuestos de esas excepciones.

El dato relativo a la salud es tratado por la Ley Orgánica 3/2018 en relación con el artículo 9 del Reglamento (UE) 2016/679 también en la Disposición adicional decimoséptima. Esta disposición y su contenido se tratará en el capítulo 3.2.2 del Título III.

1.2. Datos relativos a la salud y datos en el ámbito sanitario

1.2.1. La salud

La salud aun siento una término familiar y cotidiano no es fácil de definir. Este concepto se abordará desde tres puntos de vista, desde el punto de vista médico, desde el punto de vista integral y desde el punto de vista jurídico.

La Organización Mundial de la Salud (OMS, en inglés World Health Organitation o WHO, www.who.int/es) dependiente de las Naciones Unidas (ONU, en inglés United Nations o UN, www.who.int/es), en su Constitución aprobada en 1948, definió la salud como "es un estado de completo bienestar físico, mental y social, y no solamente la ausencia de enfermedad o dolencia"[365]. Ha habido otros intentos, pero ninguno ha logrado acaparar un abanico tan universal como el que hace esta definición.

Hay otras formas de definir la salud, para un profesional de la salud, es la que se sustenta en la biología humana, de tal forma que es la ausencia de enfermedad o la ausencia de alteración fisiológica, funcional o biológica conocida que impida o dificulte el correcto desarrollo de las funciones de los órganos, tejidos o sistemas de la persona. De esta forma la salud no se vincula a su percepción por la persona, pues esta puede o no ser consciente de esa alteración, lo cual no evita que la padezca, ejemplo de ello es la diabetes. Esta es una enfermedad crónica de la persona, cuando no ha manifestado complicaciones es frecuentemente desapercibida por quién la sufre. Otro ejemplo, pero en otro sentido, es el de una persona a la que se le ha extirpado la glándula tiroides, esta persona tuvo una enfermedad que le ocasionó la pérdida de la glándula lo cual le ha producido una alteración en su sistema hormonal, sin embargo, puede llevar una vida normal y saludable. Sin embargo, no son pocos los autores que entienden que el concepto de salud es cambiante y dependen de las personas y de los contextos desde donde se conceptualizan[366].

Para las personas la salud o estar en posesión de ella, va asociada a la sensación o idea de bienestar, mientras que la enfermedad va asociada a padecimiento, dolor, síntomas o signos, toma de tratamientos, seguimiento de dietas o el ejercicio terapéutico, así como permanencia en un centro asistencial o acudir a visitas frecuentes al médico de cabecera para una revisión corporal. Sin embargo, uno de los estados de la persona que requiere más cuidados y visitas médicas es el embarazo normal, situación fisiológica de

[365] OMS. Organización Mundial de la Salud "Quiénes somos". Disponible en https://www.who.int/es/about/who-we-are (28/02/2021).

[366] GAVIDIA, V. TALAVERA, M. (2012) "La construcción del concepto de salud". Didáctica de las ciencias experimentales y sociales,26, 161-175. p 161.

total normalidad. Para la persona estar sana es ausencia de dolor o malestar, ausencia de alteración física o funcional o ausencia de limitación de su autonomía personal.[367]

La salud está íntimamente ligada los hábitos de vida, a su medio ambiente y a su entorno social. Si para el general entendimiento de nuestro entorno lo normal es lo más frecuente, lo óptimo, lo más habitual o lo que le ocurre al 68% de un conjunto o un todo[368], para el individuo, para el ser humano la salud es la situación normal en la que se encuentra su organismo y en relación a su entorno, es la normalidad funcional de su cuerpo humano, es decir, es un resultado que se manifiesta por la existencia de equilibrio, es el resultado del funcionamiento fisiológicamente correcto de los sistemas, órganos y tejidos y de la mente de la persona, en consecuencia la salud se puede quebrar cuando dicho funcionamiento decae alterándose por causas funcionales u orgánicas, internas o externas. Es decir, si la salud es el resultado de lo normal, la falta de salud o la enfermedad es una alteración de esta normalidad y que en determinados casos deviene en la muerte, es decir, el resultado de un funcionamiento incompatible con la vida, o extremadamente anormal. Por tanto, no nos equivocamos si afirmamos que la salud es un resultado de un equilibrio.[369]

Las doctrinas más recientes y consolidadas explican que la salud y su significado, alcance y manejo, debe de verse desde la perspectiva de los factores determinantes de la salud[370] (en adelante FDS y en inglés, The determinants of health, Health Impact Assesment, HIA) que son aquellos factores sobre los que podemos actuar para proteger a salud de lesiones e incluso aquellos elementos que la puedan mejorar[371].

No se nos puede escapar la importancia que tiene la correcta búsqueda de los factores determinantes de la salud y su relación con los recursos que se utilizan para protegerla o evitar su menoscabo, en este orden de cosas, el Informe Lalonde[372], revisado ya en estas fechas[373], ya estableció en 1974 que los estilos de vida influyen en un 43% en la salud y consumen el 1,5% de los recursos, los sistemas de salud influyen en un 11% y consumen un 90% de los recursos, el medio ambiente influye en un 19% en la salud y

[367] Bestard Perelló, JJ. (2015) "La asistencia sanitaria pública". Madrid. Ed. Diaz de los Santos. p 59.

[368] En estadística y probabilidad se llama Distribución Normal, Campana de Gauss o Distribución gaussiana, a una de las distribuciones de probabilidad de variable continua que con más frecuencia aparece aproximada en fenómenos reales. Su importancia se debe fundamentalmente a la frecuencia con la que distintas variables asociadas a fenómenos naturales y cotidianos siguen, aproximadamente, esta distribución. Descubierto por Johann Carl Friedrich Gauss (1777-1855). Alemán. Matemático, astrónomo y físico.

[369] SEMI. (2021) "Salud y enfermedad ¿qué son?" Sociedad española de medicina Interna. Disponible en https://www.fesemi.org/informacion-pacientes/hemeroteca-salud/enfermedades/salud-y-enfermedad-que-son. (28/02/2021).

[370] VILLAR AGUIRRE M. (2011) "Factores determinantes de la salud: Importancia de la prevención". Acta médica peruana, 28(4), 237-241. Disponible en http://www.scielo.org.pe/pdf/amp/ v28n4 /a11.pdf. p 237.

[371] MARMOT M., WILKINSON RG. (2013) "The solid facts". Copenhagen. WHO Regional Office for Europa. Disponible en https://www.euro.who.int/data/assets/pdf_file/0005/98438/ e81384.pdf. (28/02/2021) pp 10-11.

[372] LALONDE M. (1974) "A new perspective on the health of Canadians". A working document. Otawa

[373] LALONDE M. (2002) "A new perspective on the health of Canadians: 28 years later". Rev Panam Salud Públic, 12 (3), 149-152.

utiliza un 1,6% de los recursos y la bilogía humana influye en un 27% en la salud y consume un 7,9% de los recursos.

Sin duda, los factores económicos afectan también a la salud, pero contrariamente a lo que parece inicialmente, el crecimiento económico favorece los procesos de desarrollo a largo plazo que introducen mejoras en la salud, pero una vez alcanzado cierto nivel de ingreso comienza a perjudicarse[374]. Más recientemente la Organización Mundial de la Salud (OMS/WHO) ha ido elaborando documentos, recogido evidencias y creados grupos de estudio que van permitiendo conocer los nuevos FDS o HIA que se incorporan a los ya establecidos por Lalonde en su informe. En base a los documentos de la OMS de 2013 los factores determinantes en la salud incluyen el entorno social y económico, el entorno físico y las características individuales y los hábitos de cada uno, de tal forma que la WHO estima que no se puede culpabilizar a las personas por su estado de salud, dado que es poco probable que las personas puedan controlar individualmente los factores determinantes de la salud, que sin duda, le afectan.[375]

En este orden de cosas los expertos de la WHO concluyeron en dichos documentos que estos factores incluyen los ingresos económicos familiares, el estatus social, la educación, el medio físico que incluye tanto el agua como el aire, los lugares de trabajo saludables, los edificios con sistemas reductores de accidentes, las carreteras, también influye el empleo, las condiciones de trabajo, el apoyo de redes sociales, la cultura, las creencias familiares y de la comunidad, la genética, los hábitos de vida, el nivel de conflicto personal con las frustraciones, los servicios de salud y el género, los hombres y las mujeres sufren de diferentes tipos de enfermedades en los diferentes tramos de edad. Además incorporaron un listado de factores que influyen directamente en la salud como los accidentes tanto de tráfico como los de la infancia o en los hogares, la contaminación, el ruido, efectos climáticos sobre las tierras, enfermedades transmisibles por vectores, las biotoxinas químicas, las toxinas naturales o biológicas, el plomo, el mercurio, las dioxinas, los alérgenos, la utilización de productos químicos en la agricultura, los plaguicidas, las rupturas en las cadenas de frío, los patrones dietéticos mórbiles, el alcohol, el tabaco, las llamadas drogas ilegales, microorganismos como salmonella, E.Coli, listeria, cólera, virus de la hepatitis A, B y C, el virus SARS-CoV-2, entre muchos otros, parásitos como las tricomoniasis, agentes no convencionales como el agente causante de la encefalopatía espongiforme bovina, las condiciones físicas de vida como las viviendas insalubres o la falta de vivienda, el efecto de los residuos sobre el medio ambiente, los combustibles fósiles, y las emisiones ionizantes, entre otros factores[376]. A todo ello hay que reflejar que la mayoría de los factores determinantes de la salud, cuatro quintas partes, nada tienen que ver con los sistemas sanitarios,

[374] TAPIA GRANADOS J.A. (2011) "La mejora de la salud durante las crisis económicas" España Papeles de relaciones ecosociales y cambio global, 113, 121-137. pp 133, 136.

[375] OMS (2013) La 13ª Conferencia Internacional sobre la Evaluación de Impacto en la Salud. World Health Organitation. Health Promotion Switzerland. Université de Genève. Ginebra, 2-4 de octubre de 2013.

[376] CSDH (2008) "Closing the gap in a generation: health equity through action on the social determinants of health: Commission on Social Determinants of Health final report". WHO Commission on Social Determinants of Health. World Health Organization. Geneva, Switzerland: World Health Organization, Commission on Social Determinants of Health. pp 50-179.

siendo la desigualdad social unos de los factores que mayor influencia tiene en la salud individual[377].

La salud también puede ser vista bajo el punto de vista del derecho. La vida es un bien jurídico protegido al igual que lo es la salud, artículo 43.1 de la Constitución Española, y no puede dejar de serlo, sino que además la salud está ampliamente protegida en todas las facetas de los ordenamientos jurídicos, no tan solo por la vía penal sino también por toda cuanta disciplina de derecho se cruce con elementos que puedan afectarla. Tal es el caso del ordenamiento jurídico administrativo y todo aquel que regula las relaciones de la persona con los seguros de salud, la administración sanitaria pública, los provisores de servicios y productos sanitarios. El ámbito penal, el que con más fuerza utiliza la doctrina del bien jurídico, tiene presente la salud directamente en varios de sus preceptos e indirectamente en muchos otros más. En España el Código Penal[378] entiende a la salud como dos tipos de objetos distintos, por una parte, la salud es un bien jurídico protegido principal y, por otra trata, es un bien jurídico secundario[379].

Como bien jurídico el derecho penal protege a la salud desde la perspectiva de la figura de las lesiones que son entendidas desde criterios jurídico-penales y forenses como conductas que perjudican y dañan a la salud del individuo y en concreto la integridad corporal de las personas. El régimen de responsabilidades que rige en nuestro ordenamiento jurídico, tanto en el derecho civil como en el derecho administrativo y el derecho especial[380] persiguen proteger a la salud de las personas desde la óptica de la doctrina de las obligaciones. En concreto, este régimen descansa en el hecho de la producción de alguna lesión o daño a la salud de las personas bien cuando se dan los presupuestos de la responsabilidad civil, cuando por acción u omisión se causa daño a otro interviniendo culpa o negligencia, o bien cuando la Administración incurre en supuestos de responsabilidad patrimonial, sin que deba concurrir culpa, estando ambos supuestos obligados a reparar el daño causado.

En este orden de cosas, si la salud es un bien jurídico protegido, tiene mucho sentido que los datos de las personas relativos a su salud también se cobijen bajo esta protección, además de las razones que la normativa de protección de datos esgrime al referirse que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, Considerando uno del Reglamento (UE) 2016/679.

1.2.2. El paciente, el enfermo y el usuario de servicios sanitarios

El significado de los conceptos paciente, enfermo y usuario de un servicio sanitario no debe entenderse como un mero ejercicio teórico o académico, sino que ayuda a poder

[377] SEGURA BENEDICTO A. (2014) "Recortes, austeridad y salud". Gaceta Sanitaria, 28 (1), 7-11. p 10.

[378] Ley Orgánica 10/1995, de 23 de diciembre, del Código Penal.

[379] BESTARD PERELLÓ, JJ. (2015) "La asistencia sanitaria …..". Op.cirt; pp 38-50.

[380] Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias modificado por la Ley 3/2014, de 27 de marzo.

entender y a identificar el dato de la persona física relativo a cuestiones de salud y a distintos escenarios.

No es infrecuente leer expresiones tales como “los datos del paciente”, “los datos de la historia clínica” o los “los datos de salud” y no es tampoco infrecuente que se entienda como tal, solo a los datos de un enfermo, lo cual es una simplificación errónea.

La Real Academia Español define la expresión paciente cuando esta se utiliza como sustantivo a persona que está bajo examen o tratamiento médico, y añade, es común en cuanto al género.

Según Cambridge Dictionary, la expresión paciente, que en inglés es patient, tiene el siguiente significado: a person who is receiving medical care, or who is cared for by a particular doctor or dentist when necessary (una persona que recibe atención médica, o que es atendida, cuando es necesario, por un médico o dentista).

Para la Ley 41/2002 paciente es la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de su salud, artículo 3 de la Ley 41/2002.

Sin embargo, si bien todos los datos del paciente pueden ser o son relativos a su salud, no todos los datos de una persona física relativos a su salud son atribuibles a que esta persona sea paciente o que sea atendida por un médico o por un servicio sanitario.

En este orden de cosas un paciente, palabra sin género, es quien acude a un servicio sanitario para ser examinado o tratado por un profesional de la salud y no necesariamente un médico, pues, el profesional que le atiende no debe ser necesariamente un médico pues la persona atendida puede estar en proceso de diagnóstico a través de los técnicos o haber sido ya diagnosticada y estar tan solo en proceso aplicación terapéutica a través de algún otro profesional de la salud.

Una persona puede acudir a un centro asistencial por sentirse indispuesta, con dolor o con sensación de malestar y que el médico, tras el examen y diagnóstico, concluya que está perfectamente sana. Esta persona durante el tiempo que estuvo asistida por el médico o el servicio sanitario era también considerada un paciente. Otro ejemplo lo tenemos con las mujeres en proceso de embarazo, estando sanas son atendidas por su médico y por el sistema sanitario, y que, aunque disponen de su historia clínica, no son consideradas como pacientes.

Por otra parte, una persona que acude a un profesional de la salud no tiene que haber acudido necesariamente por una dolencia o enfermedad. Según la Encuesta Nacional de Salud de 2017 en España realizada por el Ministerio de Sanidad, Consumo y Bienestar Social[381] en relación a las consultas al médico de cabecera, el 12,91% se debió a motivos administrativos y el 9,21% a otros motivos no médicos. En la franja de edad anterior a

[381] MS. Ministerio de Sanidad (26 junio 2018). “Encuesta Nacional de Salud España 2017” Ministerio de Sanidad, Consumo y Bienestar Social. Madrid. Disponible en https://www.mscbs.gob.es/estadEstudios/estadisticas/encuestaNacional/encuesta2017.htm (31/05/2021).

los 15 años, el entre un 30 y un 46 % de las visitas al pediatra es en relación al programa del niño sano.

Otros casos de acceso a los servicio de un profesional médico en personas no-enfermas o asintomáticas, pertenecen a personas que son sometidas a reconocimientos rutinarios bien en el escenario laboral, bien en el escenario de algunos supuestos que requieren un certificado médico, como las pruebas de aptitud para el carnet de conducción de vehículos, o bien en el escenario escolar mediante los reconocimientos de salud escolar, por nombrar algunas de las situaciones posibles en las que una persona física acuda a ser examinada por un médico por no motivos de quebrantamiento de su salud sino por motivos de programas preventivos o simplemente para tomar nota de sus parámetros corporales o por el requerimiento de un tercero.

Para la Ley 41/2002 la persona que utiliza los servicios sanitarios de educación y promoción de la salud, de prevención de enfermedades y de información sanitaria es un usuario, artículo 3 de la Ley 41/2002.

Cuando las personas acuden a vacunarse como causa de un programa de vacunación o por voluntad propia, estas personas no son estrictamente pacientes pues no acuden a los servicios sanitario como causa de ninguna dolencia, ni buscan ningún tipo de examen médico, si buscan tratamiento para ningún tipo de dolencia, sino lo que busca es una acción o intervención de carácter sanitario para prevenir una enfermedad[382].

Enfermo o enferma, es la expresión que se utiliza para aquella persona que padece una enfermedad, sea esta aguda o crónica. En este orden de cosas, se entiende por enfermedad según la Organización Mundial de la Salud (OMS), como: “la alteración o desviación del estado fisiológico en una o varias partes del cuerpo, por causas en general conocidas, manifestada por síntomas y signos característicos, y cuya evolución es más o menos previsible”[383].

Se entiende que hay enfermedades endógenas, enfermedades exógenas, enfermedades medioambientales y mixtas. Con carácter general las enfermedades están catalogadas mediante la Clasificación Internacional y Estadística de Enfermedades y Problemas Relacionados con la Salud (CIE), que es una lista de códigos publicada por la Organización Mundial de la Salud. La CIE es una clasificación central en la Familia de Clasificaciones

[382] OMS (2021) “Vacunas e inmunización: ¿qué es la vacunación?”. Organización mundial de la salud. Disponible en https://www.who.int/es/news-room/q-a-detail/vaccines-and-immunization- what-is-vaccination?adgroupsurvey={adgroupsurvey}&gclid=Cj0KCQjwi7yCBhDJARIsAMWFScP4WVF8N3UJoZxMLdSWgCqNXy60u1UDPNgOv6YWNQOd6X0lmaNTSWAaArglEALw_wcB (28/02/2021).

[383] HERRERO JAÉN, S. (2016). “Formalización del concepto de salud a través de la lógica: impacto del lenguaje formal en las ciencias de la salud”. Santa Cruz de la Palma. ENE Revista de Enfermería, 10(2). Disponible en http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1988-348X2016000200006 (31/01/2021).

Internacionales de la OMS (en inglés, WHO-FIC). Bajo revisión permanente, la CIE actualmente en uso es la décima edición CIE-10[384].

Sin embargo, todas las enfermedades no afectan de igual forma a todos los pacientes dado que su estado de afectación o gravedad está vinculado a la edad, a las patologías o situaciones concomitantes, a parámetros biofísicos, al consumo de tóxicos, a los hábitos de vida, a los antecedentes patológicos y a la idiosincrasia de la persona.

Los datos que serán utilizados y ayudaran al profesional a conocer el estado de salud de una persona son muchos y su listado sería farragoso y no es motivo de este estudio, pero con carácter meramente orientativo los siguientes datos dan información sobre el estado de salud la persona: la verbalización y utilización de la palabra, pliegues faciales, observación de prótesis externas o lentes, altura, peso, estado de tronco y extremidades, integridad y coloración de la piel y mucosas, estado o situación de los anexos a la piel, las pupilas, movilidad ocular, movilidad y deambulación, orientación, estado de atención, temperatura corporal, tensión arterial, frecuencia cardiaca, capacidad vital inspiratoria, análisis de fluidos corporales, análisis de imágenes internas del cuerpo, etc.

Cabe preguntarse si todo enfermo o enferma es paciente independientemente de que sea atendido por un profesional sanitario. Esta pregunta tiene una respuesta, una persona enferma o un enfermo será un paciente cuando reciba atención médica o sanitaria. Por tanto, todos los datos de la persona enferma serán susceptible de ser considerados datos relativos a la salud y en especial cuando estos datos hagan referencia a su dolencia, directa o indirectamente, o sean utilizados en algún centro asistencial.

Los datos de una persona enferma pueden hacer referencia a su capacidad o incapacidad, física mental o legal, en cuyo caso tendrán que ver con datos relativos a su salud. También son datos relativos a la salud de una persona aquellos que hagan referencia a su estado de curación, pues este es posterior al de enfermedad y, en muchos casos, consecuencia de un tratamiento. De esta forma no todos los pacientes están enfermos, ni todos los enfermos son pacientes.

El supuesto de una persona que interactúa con algún servicio sanitario, de forma voluntaria o involuntaria, directa o indirecta, pero que no es una persona enferma ni un paciente, entonces esta persona es un usuario del sistema sanitario, bien sea de forma pasiva o activa.

Por último, caben casos especiales de personas que bien se encuentran en bases de datos sanitarios o en las cuales constan sus datos sanitarios pero que a su vez no han sido tan siquiera usuario sistema sanitario. Estos son el caso, por una parte, de los estudios de investigación y también el caso de los estudios epidemiológicos y, por otra parte, de las bases de datos de compañías de seguros.

[384] MS. Ministerio de Sanidad (2020). eCIE10ES. Edición electrónica de la CIE-10-ES Diagnósticos. 3ª Edición-Enero 2020. Actualización Julio 2020. Disponible en https://eciemaps.mscbs.gob.es/ ecieMaps/ browser/ index_10_mc.html (31/01/2021).

1.2.3. Dato cualificado. El dato personal en el sector sanitario y el dato personal relativo a la salud. La cualificación de un dato

El concepto de dato no está suficientemente definido y actúa en las relaciones humanas y de comunicación más como un concepto intuitivo que como un concepto concreto y tasado. Sin embargo, esta dificultad no es razón por la cual no se deba extremar la concreción del término dato con el fin de acotar lo que podría entenderse por una cierta inseguridad jurídica.

Los datos sanitarios son considerados por la jurisprudencia del Tribunal Supremo del año 2000[385] como datos de carácter personal y no como datos personales[386]. Sin embargo, desde que la nueva legislación en protección de datos ha abandonado la expresión datos de carácter personal, no cabe ningún tipo de confusión.

Ocurre lo mismo con el concepto de dato de salud o dato personal sanitario o dato sanitario de carácter personal o dato personal de naturaleza sanitaria. El ordenamiento jurídico no lo define, si bien Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos ofrece una definición que dice que *la* expresión "datos médicos" se refiere a todos los datos personales relativos a la salud de un individuo. Se refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos.

El dato personal relativo a la salud o dato de la salud de una persona, como no es difícil de adivinar, tiene que ver directamente con su estado de salud de esa persona. Un simple dato sobre la tensión arterial, sobre la temperatura corporal, sobre los sonidos de una auscultación o sobre la tasa de la hormona gonadotropina coriónica (HCG) en orina, son datos claramente relativos a la salud de la persona titular de los mismos o persona de la cual emanan los sonidos de la auscultación o de la persona que miccionó la orina analizada.

Para la AEPD los datos relativos a la salud se definen como: "los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud"[387].

Sin embargo, a pesar de la definición de la AEPD, la experiencia en los hospitales y centros de salud demuestra que datos de salud o relativos al estado de salud de una persona son todos aquellos que emanan de la observación o exploración de su cuerpo o del análisis se sus fluidos dentro unos rangos o valores, lo cual permitirá que un profesional pueda discernir si dichos datos o cifras están dentro de la franja de lo que se entiende como normalidad o están fuera y hacen a la persona subsidiaria de poder padecer una patología o alteración, además de los datos necesarios para poder realizar la prestación o atención sanitaria.

Los datos de salud o relativos al estado de salud, están protegidos por el artículo 9 del Reglamento (UE) 2016/679 y por el artículo 9 de la Ley Orgánica 3/2018.

[385] STS 6188/1996, 31 de octubre del 2000 (Sala de lo Contencioso), FD 2º.

[386] *Vid Supra p 30* capítulo 1.3. del Título I.

[387] AEPD (2019) "Guía para pacientes y usuarios de la sanidad". Diciembre 2019. Disposición en https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf (28/02/2021).

1.2.3.1. Dato de la salud de la persona sana y dato de la persona enferma

En este orden de cosas, como ya se ha apuntado hay que incluir como dato de salud no tan solo a los datos de personas enfermas, pues una persona puede ser observada o explorada o se le pueden analizar sus fluidos y no estar enferma y ni siquiera estar en proceso de diagnosis, tal es el caso de un trabajador al cual se le realiza un reconocimiento médico o tal es el caso de una persona que recibe una vacuna. El trabajador no acudió al servicio médico necesariamente por sentirse mal o la persona no acudió al servicio de salud necesariamente por estar enferma sino para no estarlo.

El dato personal de salud no implica el dato de una persona enferma, por otra parte, hay datos relativos a la salud que poco tiene que ver con observaciones corporales o análisis de fluidos. Datos personales no relativos a la salud de la persona son recabados en los centros sanitarios bien por indicaciones administrativas o bien por criterios médicos.

De la práctica clínica de un profesional de la salud en cualquier centro sanitario se deduce que para la atención de una persona que acude a un médico para saber si un signo o síntoma es causado por una enfermedad o no, el médico o el profesional sanitario puede necesitar saber sobre circunstancias personales que nada tienen que ver con el síntoma o signo referido y que los hará constar en la historia clínica. Por ejemplo, los antecedentes familiares, la profesión o el trabajo o las condiciones laborales pueden ser datos necesarios dentro del proceso de diagnosis. Frente a un eritema o rubicundez de la piel, el saber que la persona trabaja en la construcción puede ayudar a encauzar las sospechas diagnosticas[388]. Otro ejemplo clarificador es el dato que hace referencia a los hábitos de las personas. Conocer el hábito alimenticio o la dieta de una persona no deja de ser un dato de la persona que no permite su identificación[389], pero cuando este dato es recabado por un profesional de la salud con la intención de utilizarlo en el proceso diagnóstico o terapéutico e incluirlo en la historia clínica, entonces se convierte en un dato personal relativo a la salud.

El dato de salud de la persona sana y el dato de salud de la persona enferma, como es obvio, son datos personales relativos a la salud de la persona, están protegidos por el artículo 9 del Reglamento (UE) 2016/679 y por el artículo 9 de la Ley Orgánica 3/2018.

1.2.3.2. Dato personal en el contexto sanitario

Está claro que el dato de la dieta o el relativo a la profesión de una persona o a las condiciones de trabajo no es aisladamente un dato de salud, pero dado que este dato se solicitó y tomó durante un proceso asistencial se considera, en el contexto del centro asistencial, un dato sanitario. Pero incluso tal como dice el Considerando 35 del Reglamento 2016/679, los datos de inscripción en un centro sanitario son datos relativos

[388] MS. Ministerio de Sanidad (25 febrero 2003) "Dermatosis laborales". Protocolo de vigilancia sanitaria específica. Comisión de salud pública. Consejo Interterritorial del Sistema Nacional de Salud. Disponible en https://www.mscbs.gob.es/ciudadanos/saludAmbLaboral/docs/dermatos.pdf (28/02/2021).

[389] SACYL (2021) "Dieta mediterránea" Portal de salud. Consejería de Salud de Castilla y León. Disponible en https://www.saludcastillayleon.es/es/enfermedades-problemas-salud/enfermedad-cardiovascular/prevencion- habitos-vida-saludables/dieta-mediterranea (28/02/2021).

a la salud, pues el Considerando 35 amplia el espectro y entiende incluso como dato personal relativo a la salud "la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria".

La cualificación de dato personal relativo a la salud puede ser una cualificación sobrevenida. En este orden de cosas, la lectura del Considerado 35, así nos lo hace notar:

> "El Considerando 35 dice: Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro."

Los datos personales no relativos a la salud pueden adoptar el rango de datos relativos a la salud, cuando estos datos han sido utilizados en un entorno sanitario. Este tipo de datos están protegidos por el artículo 9 del Reglamento (UE) 2016/679 y por el artículo 9 de la Ley Orgánica 3/2018.

1.2.3.3. Dato personal en el ámbito del secreto profesional sanitario

Se puede analizar, también el alcance del concepto dato relativo con la salud bajo otra óptica. Por ejemplo, una de estas es la vertiente del secreto profesional del médico en el sentido de que todo lo que se le cuenta al médico en el proceso asistencial es considerado materia reservada al secreto profesional y en consecuencia dato sanitario. En este orden de cosas la Asociación Médica Mundial de 1948 definió que "es la obligación ética del médico de no divulgar ni permitir que se conozca la información que directa o indirectamente obtenga sobre la salud y vida del paciente".

Nos encontramos ante una cualificación sobrevenida, como en el punto anterior, un dato personal no relativo a la salud y no protegido por el artículo 9 del Reglamento (UE) 2016/679 pasa a tener la consideración de datos personal relativo a la salud y en consecuencia pasa a estar protegido por el artículo 9 del Reglamento (UE) 2016/679.

Esta situación o acción calificadora es el secreto profesional. El secreto médico, dentro del derecho a la intimidad, es la obligación permanente del médico en cualquier relación profesional[390].

[390] GONZÁLEZ DE LA PEÑA A.S. (2017) "El secreto del profesional sanitario: Limitaciones y Singularidades", V Promoción Máster en Derecho Sanitario Universidad San Pablo CEU. Madrid. pp 7-8.

Sin embargo, pese a la importancia del hecho lo cierto es que el secreto profesional no está regulado en España, pese a que el artículo 24 de la Constitución Española de 1978 dice que la ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos.

Los datos personales no relativos a la salud sometidos al secreto profesional adquieren la protección del 9 del Reglamento (UE) 2016/679 y por el artículo 9 de la Ley Orgánica 3/2018 y se convierte, a efectos del RGPD, en datos personales relativos a la salud.

1.2.3.4. Dato personal relativo a la salud o dato relativo a la salud

El Reglamento (UE) 2016/679 en su artículo 4, definiciones, define como dato relativo a la salud como como aquellos datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

La Ley Orgánica 3/2018 no utiliza la expresión dato/s relativo/s a la salud ni dato/s personal/es relativo/s a la salud, sino que utiliza la expresión datos de salud.

La Agencia Española de Protección de Datos entiende en su publicación Protección de Datos "guía para el ciudadano", la definición de datos relativos a la salud como aquellos datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. La definición que utiliza la AEPD para los datos relativos a la salud es la misma que utiliza el Reglamento (UE) 2016/679. Si embargo, nada dicen sobre el espacio temporal, pero se sobreentiende que se refiere al estado de salud pasado o presente.

Los datos personales relativos a la salud o datos relativos a la salud son los que de forma explícita cita el 9 del Reglamento (UE) 2016/679 y por el artículo 9 de la Ley Orgánica 3/2018 y se convierte, a efectos del RGPD.

1.2.3.5. Dato relativo a la salud, dato clínico e información clínica

Una vez visto el concepto de dato personal relativo a la salud y sus distintas formas de cualificación y determinación, es preciso tratar el dato relativo a la salud por excelencia, es decir, la información clínica.

La información clínica de cada persona es propiedad de quién la genera y los derechos sobre dichos datos vienen determinados por la Ley 41/2002 y también por Ley Orgánica 3/2018. El paciente tiene el derecho de acceso a la documentación clínica y a obtener copia de los datos que figuran en ella, en base a la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (en adelante, también Ley 41/2002). Estos derechos también aparecen de forma no especifica sino genérica en el Capítulo III, sobre los derechos del interesado, del Reglamento (UE) 2016/679 y en el Título III de la Ley Orgánica 3/2018. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos.

En relación a los datos especialmente protegidos relativos a la salud de los pacientes, a datos genéticos o datos biométricos debemos entrar a valorar el dato clínico, la información clínica, información asistencial, la historia clínica y la documentación clínica.

El dato en el ámbito de la salud suele atender a la denominación de dato clínico, aunque no siempre tienen que ver con datos producto de una alteración, sino que son todos los datos que se acopian de una persona durante el proceso de atención sanitaria. Así pues, el dato clínico son también los datos sobre su estado físico o sobre su salud de manera leal y verdadera que tiene la persona el deber de facilitar por razones de interés público o con motivo de la asistencia sanitaria, así como el de colaborar en su obtención, especialmente cuando sean necesarios, artículo 2.5 de la Ley 41/2002.

El dato clínico es todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de la persona en cuestión[391], o la forma de preservarla, cuidarla, mejorarla o recuperarla que conforma la documentación clínica y que a su vez a lo largo del proceso asistencial en su conjunto conforma la historia clínica del paciente, artículo 3 de la Ley 41/2002. Los datos referentes a la salud de la persona son aquellos que adquieren el derecho de confidencialidad y privacidad de acceso, es decir, los que para su acceso se requiere amparo legal, artículo 7 de la Ley 41/2002, debiendo añadir el deber de secreto que sobre ellos están obligados los que tengan acceso a ellos por motivos profesionales, artículo 16.6 de la Ley 41/2002.

Los datos son subsidiarios de que sobre ellos y para su acceso, los centros sanitarios "como conjunto organizado de profesionales, instalaciones y medios técnicos que realiza actividades" del artículo 3 de la Ley 41/2002, están obligados a adoptar las medidas oportunas elaborando, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes.

La información clínica es todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla, artículo 3 de la Ley 41/2002. La información clínica, formando parte de todas las actuaciones asistenciales, artículo 4.2 de la Ley 41/2002, es el conjunto de datos recopilados y ordenados que ha generado la persona a través de una determinada atención sanitaria bien por haber sido solicitada por ella misma o por quien la representa o bien, sin su consentimiento, por necesidad vital.

A todo esto, la Ley no tan solo reconoce al dato y a la información clínica como objetos de protección especial, sino que hace al paciente (o usuario) titular único de los derechos de información que sobre él están en el centro sanitario y de toda la información clínica que

[391] HUERTA ARAGONES, J. CELA DE JULIAN, E (2 febrero 2018) "Hematología práctica: interpretación del hemograma y de las pruebas de coagulación". 15º Curso de actualización en pediatría. AEPap Disponible en file:///C:/Users/Juan%20J/Documents/TRABAJO%20DE%202021/DOCTORADO%202018/ TRABAJOS %20SOBRE%20LA%20TESIS/REDACCION%20DOCUMENTO/NUEVA%20VERSION%20TESIS/VERSIONES %20MODIFICADAS%20POR%20BLANCA/BILBLIOGRAFIA%20TESIS/ HUERTA%2020PG.pdf (28/02/2021).

obra en manos de terceros. La ley refuerza esta titularidad pues es su autorización la que permite que esta información se accedida legalmente por personas vinculadas por razones familiares, o de hecho, al sujeto afectado, artículo 5.1 de la Ley 41/2002.

A los efectos de la teoría del dato y los mecanismos de protección de los mismos se entiende que información clínica e información asistencial es prácticamente lo mismo, si bien para algunos la información clínica está más relacionada con el acto médico y los procedimientos de enfermería que la información asistencial que tiene un espectro más amplio y es relativo a cualquier dato del paciente o usuario durante su estancia en el centro sanitario o durante su atención y cuidado.

Informe de alta médica es el documento emitido por el médico responsable, en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas. Todo paciente, familiar o persona vinculada a él, en su caso, tendrá el derecho a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial, un informe de Alta.

1.2.3.6. Dato cualificado, propiamente. La cualificación de un dato

El dato de la persona, sin más, está protegido por el Reglamento (UE) y por la Ley Orgánica 3/2018 mediante la regulación de su tratamiento.

La normativa de protección del dato de la persona contempla en el artículo 9 del Reglamento (UE) 2016/679, de tratamiento de categorías especiales de datos personales, la prohibición del tratamiento de ciertos tipos de datos, a los cuales los engloba en categorías especiales de datos personales. El artículo 9.1 incluye en el listado de datos personales de tratamiento prohibido a los “datos relativos a la salud”.

Por otra parte, cuando un dato personal cualquiera entra en contacto, de la mano de la persona afectada o sin su participación, con el sector de la salud o el sector sanitario, de forma activa o de forma pasiva, o es la causa que obliga a una tercera persona al secreto profesional, sanitario, se convierte en un dato cualificado porque sin ser un dato de naturaleza sanitaria se asimila al dato relativo a la salud protegido especialmente por el artículo 9 del Reglamento (UE).

Así se pronuncia el Considerando 35 del Reglamento (UE) 2016/679 al entender que entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado, los recogidos con ocasión de su inscripción a efectos de asistencia sanitaria o con ocasión de la prestación de tal asistencia, todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios, el riesgo de padecer enfermedades, todo ello independientemente de su fuente.

De tal forma que entendemos, en el contexto de esta Tesis, por dato cualificado como aquel dato que, sin tener una naturaleza especial o sin pertenecer a ninguna categoría especial de datos que lo haga susceptible de ser considerado un dato de tratamiento prohibido, se emite en un determinado escenario, situación o lugar y por este hecho

adquiere las restricciones propias del tratamiento de los datos de categoría especial del artículo 9 del Reglamento atribuibles a los datos relativos a la salud.

Con carácter general, los datos cualificados son siempre datos asimilables a los datos personales relativos a la salud, protegidos por el Reglamento (UE) 2016/679 y por el artículo 9 de la Ley Orgánica 3/2018.

Las vías de calificación de un dato en dato relativo a la salud son:

1. Entrar en contacto con el sector de la salud.
2. El secreto profesional.

1.2.4. Los datos relativos a la salud

La propia naturaleza del estudio nos obliga a tratar amplia y específicamente el dato en el sector de la salud. El ámbito del estudio obliga al investigador a tratar todos los aspectos que puedan intervenir directa o indirectamente en la cuestión sometida a análisis, siendo indudable que hablar de sanidad y no hacerlo de su materia central, concepto esencial, es del todo insuficiente.

Todo ello nos lleva a dedicar este capítulo 1.2. del Título III a los datos de la salud en su sentido más amplio y extenso. Una vez que ya se ha definido qué es o qué se entiende por salud, una vez que se ha explicado al concepto de usuario de los servicios sanitarios entendido como paciente, pero también a aquel usuario del servicio que no se considera paciente, una vez que se ha tratado al dato sanitario como dato cualificado, es preciso dar entrada al dato relativo a la salud, propiamente dicho.

Lo datos relativos a la salud aparecen inicialmente en la Ley de 1992 dentro de artículo denominado datos especialmente protegidos, para luego entre 1995 y 2016 aparecer como datos dentro de las categorías especiales de datos.

La expresión datos relativos a la salud no aparecen en el texto del año 2018, la Ley Orgánica 3/2018, si bien implícitamente se entienden incluidos pues refiere el artículo 9 al artículo 9 del Reglamento (UE).

El RGPD, artículo 4.15 y Considerando 35 conforma un concepto muy amplio de dato de salud. Como novedad incluye los números, símbolos o códigos que identifiquen a la persona a efectos sanitarios [392].

El tratamiento del dato personal relacionado con la salud de las personas está prohibido por el artículo 9 del Reglamento (UE) 2016/679, pero esta prohibición está regulada por el apartado 2 en sus puntos h) e i) y por el punto j), tal como ya se ha tratado en el capítulo 1.1. del Título III.

De alguna forma los aspectos relativos con la salud están muy condicionados por la alta especialización de todas las materias relativas a la medicina lo cual provoca una cierta asimetría de la información entre persona/paciente y profesional de la salud y esta

[392] BELTRÁN AGUIRRE, JL (2018) "Reglamento general …..", op.cit; pp 74-76, p 76.

característica también favorece una especial tutela por parte del derecho[393]. Esta asimetría afecta al usuario en un sentido amplio, incluso en sus derechos, "el paciente no conoce sus derechos"[394].

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, dedica a los datos personales relativos a la salud y su tratamiento, el artículo 9, de categorías especiales de datos, y la Disposición adicional decimoséptima, sobre tratamientos de datos de salud.

Esta disposición décimo séptima mediante su punto 1 crea lo que se podría denominar el *sistema de protección de datos relativos a la salud* en España, al remitir la ley a la siguiente red normativa o sistema normativo:

1. La Ley 14/1986, de 25 de abril, General de Sanidad.
2. La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
3. La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
4. La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
5. La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
6. La Ley 14/2007, de 3 de julio, de Investigación biomédica.
7. La Ley 33/2011, de 4 de octubre, General de Salud Pública.
8. La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
9. El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.
10. El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

1.2.5. Los datos en el sector sanitario

Los datos en el sector sanitario son muy abundantes, hay datos relativos a las personas y datos independientes de las personas, aunque con los procesos de contabilidad analítica y asignación de costes a procesos, cada día más frecuentes, se van vinculando de forma progresiva los datos de actividad a los datos económicos y los datos de actividad están inherentemente vinculados a los datos de las personas.

En el sector sanitario la mayor parte de los datos de las personas pertenecen a los datos cualificados vistos en el capítulo.1.2.3. del Título III, a los cuales se le aplica el tratamiento de la categoría de especial de datos relativos a salud, en base a la definición que ofrece el Reglamento (UE) 2016/679.

[393] *Vid. Supra 253* capítulo 1.1 del Título III.

[394] MEDINACELI DÍAZ, K.I. (2016) "El tratamiento de los datos …..", op.cit; p 522.

Los datos relativos a la salud de las personas, propiamente dichos, y considerados muchos de ellos como datos clínicos, en los centros sanitarios se organizan entorno a la historia clínica, a la tarjeta sanitaria y a la receta, aunque también existen otros documentos como son los certificados, las agendas de los centros sanitarios, entre otros, sustentados exclusivamente por datos relativos a la salud de las personas y que no están incluidos en la historia clínica.

También se organizan los datos relativos a la salud y los datos cualificados de las personas en torno al Conjunto Mínimo Básico de Datos, que será tratado en este apartado.

En los siguientes subapartados se describirán las historias clínicas, las tarjetas sanitarias, las recetas y el Conjunto Mínimo Básico de Datos.

1.2.5.1. La historia clínica

El paradigma del dato sanitario o dato personal sanitario (o dato relativo a la salud o lo que algunos incluso llaman como dato de salud), es sin duda la historia clínica, regulada en Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[395].

La historia clínica es el término que por excelencia se utiliza en relación a la información que sobre una persona se trata en un centro sanitario siendo un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente por lo que los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste, como instrumento fundamental para su adecuada asistencia y para la continuidad de la misma, artículo 16 de la Ley 41/2002.

En historia clínica deberá constar como mínimo, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley, a su vez, constará la voluntad del paciente de no ser informado, en su caso, lo cual no impediría la función propia e inherente de la historia clínica. En la historia clínica constará como mínimo toda la información que se proporcione verbalmente y dejando constancia, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias, artículo 4 de la Ley 41/2002.

La historia clínica comprende el conjunto de documentos que contienen los datos clínicos y personales no clínicos (cualificados), valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, artículo 3 de la Ley 41/2002, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro, artículo 14 de la Ley 41/2002.

[395] HILDALGO CEREZO, A. (2016) "Protección de datos de carácter personal relativos a la salud del paciente: fundamentos, protección a la intimidad y comentarios al Reglamento UE 2016/679". Revista de Derecho UNED, 19, 715-744. Disponible en http://revistas.uned.es/index.php/ RDUNED/ article/ viewFile/ 18462 / 15501 (28/02/2021). pp 736 y 738.

La historia clínica tendrá como fin principal facilitar la asistencia sanitaria y su continuidad, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. En realidad, es un "documento médico con implicaciones jurídicas, o dicho de otra manera constituye un documento médico legal"[396].

El contenido mínimo de la historia clínica será, artículo 15 de la Ley 41/2002, (en cada Anexo hay un caso real): la documentación relativa a la hoja clínico-estadística (Anexo I), la autorización de ingreso (Anexo J), el informe de urgencia (Anexo K), la anamnesis (Anexo L) y la exploración física (Anexo M), la evolución (Anexo N), las órdenes médicas (Anexo O), la hoja de interconsulta (Anexo P), los informes de exploraciones complementarias (Anexo Q), el consentimiento informado (Anexo R), los informe de anestesia (Anexo S), el informe de quirófano o de registro del parto (Anexo T), el informe de anatomía patológica (Anexo U), la evolución (Anexo V) y planificación de cuidados de enfermería (Anexo W), la aplicación terapéutica de enfermería (Anexo X), el gráfico de constantes (Anexo Y) y el informe clínico de alta (Anexo Z).

En la historia clínica del paciente, además, quedará constancia razonada de las anotaciones relacionadas con las Instrucciones Previas del artículo 11.3 de la Ley 41/2002.

En la historia clínica de un paciente hospitalario son solo exigibles los documentos necesarios para la hospitalización. Cuando se trate del nacimiento, la historia clínica incorporará, además de la información a la que hace referencia este apartado, los resultados de las pruebas biométricas, médicas o analíticas que resulten, en su caso, necesarias para determinar el vínculo de filiación con la madre, en los términos que se establezcan reglamentariamente, artículo 15.3 de la Ley 41/2002.

La gestión, archivo, seguridad, conservación y recuperación de las historias clínicas de los pacientes corresponde a cada centro sanitario. De tal forma que la ley determina que es cada centro sanitario en particular y no la Administración sanitaria de la Comunidad Autónoma, la responsable. Así pues, establece que las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental, artículo 14 de la Ley 41/2002.

La responsabilidad de cada centro lo es en cualquiera de los formatos que tenga la historia clínica, de tal forma que la ley 41/2002 determina en su artículo 14.2 que cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

[396] SISO MARTIN, J (18 y 19 abril 2017) "La historia clínica. Su importancia en el proceso de responsabilidad sanitaria y su valor como medio probatorio". Curso "Responsabilidad sanitaria y la nueva configuración legal de la imprudencia médica". Disponible en http://www.juansiso.es/ Almacen/ HISTORIA %20CLINICA%20Y%20SU%20IMPORTANCIA%20EN%20EL%20PROCESO%20DE%20RESPONSABILIDAD%20SANITARIA.pdf (28/02/2021). p 15.

EL Tribunal Supremo en la sentencia de la Sala de lo Contencioso-Administrativo 3006/2010, de 2 de junio de 2010[397], reconoce al responsable de su custodia en lo relativo a la hoja rosa "Historias de urgencias" que queda en poder del facultativo al realizar la asistencia y luego bajo la responsabilidad de la sociedad que gestiona el centro asistencial. El Tribunal Supremo confirmó la multa de 300.506,05 euros impuesta por la Agencia Española de Protección de Datos en 2005 a una sociedad toco-ginecóloga que prestaba servicios a la clínica sevillana Sagrado Corazón por arrojar a la basura 158 historias clínicas con datos personales de pacientes.[398]

La responsabilidad de la historia clínica rece sobre dos figuras, por una parte, sobre el facultativo que atiende al paciente, y, por otra parte, sobre en centro sanitario en todo lo que sea su gestión, archivo, seguridad, conservación y recuperación de las historias clínicas. El responsable del centro sanitario es el director gerente. Sobre esta figura cada Comunidad Autónoma ha dictado su normativa, sin embargo, en todos los casos sigue el espíritu y fin del Real Decreto 521/1987, de 15 de abril, por el que se aprueba el Reglamento sobre Estructura, Organización y Funcionamiento de los hospitales gestionados por el Instituto Nacional de la Salud. El artículo 6 de dicho Real Decreto entiende que en la Gerencia del centro sanitario recae la representación del hospital y la superior autoridad y responsabilidad dentro del mismo.

El desarrollo de este capítulo 1.2.5.1. sobre la historia clínica se desarrollará mediante los siguientes subapartados:

- Los códigos de identificación de la historia clínica.
- El informe de Alta.
- Otros documentos clínicos en el Sistema Nacional de Salud.
- La historia clínica digital en el Sistema Nacional de Salud.

1.2.5.1.1. Los códigos identificativos de la historia clínica

Cada historia clínica está dotada de un número propio que genera cada centro sanitario. Cada historia clínica en un centro sanitario es única para cada paciente, en la cual aparecen todas las veces que el paciente ha sido atendido en el hospital por inicial o por otra a causa distinta de la inicial, denominándose episodio a cada nuevo proceso clínico.

La historia clínica se vincula con la tarjeta sanitaria Individual a través del Código de Identificación Personal, el cual constará en la Base de datos de población protegida del Sistema Nacional de Salud.

[397] STS 3006/2010 de 2 de junio (Sala de lo Contencioso), FD 1º.

[398] EL MUNDO (26 AGOSTO 2010) “Multa de 300.000 euros por tirar a la basura historias clínicas de 158 pacientes ginecológicas”. Disponible en https://www.elmundo.es/ elmundo/ 2010/08/26/ andalucia_sevilla/ 1282812502.html (31/01/2021).

El código de identificación de la historia clínica es un dato que permite la identificación de la persona y de sus datos relativos a su salud, es un dato identificativo en base a lo comentado en el capítulo 1.3 del Título I[399].

1.2.5.1.2. El informe de alta

El informe de Alta en España aparece en el ordenamiento jurídico por primera vez en el año 1984, a través de Orden de 6 de septiembre de 1984, mediante la cual se establecía su obligatoriedad en centros públicos y privados. Sin duda considerado un gran avance tanto en el ámbito de la gestión sanitaria como en el ámbito del derecho sanitario.

En artículo 3 de dicha norma se establecen los requisitos mínimos que deben constar en un Informe de Alta:

- Referidos a la identificación del centro sanitario y unidad asistencial.
- Referidos a la identificación del paciente.
- Referidos al proceso asistencial.

En la actualidad el informe de alta está regulado por el Capítulo VI, artículos 20 a 23, y por la Disposición transitoria única de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

El Informe de Alta es el documento emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas. Es preciso detenerse en este punto y hacer notar que el Informe de Alta, aunque tiene la indicación terapéutica no sustituye en ningún caso la función de la receta médica.

Todo paciente, familiar autorizado o persona autorizada vinculada al o a la paciente, en su caso, tendrá el derecho a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial el informe de alta. Las características, requisitos y condiciones de los informes de alta se determinarán reglamentariamente por las Administraciones sanitarias autonómicas.

Se debe destacar la gran importancia que tiene el informe de alta para la calidad de la actividad asistencial para el colectivo de los profesionales sanitarios.[400]

[399] En la p 29 de esta Tesis consta: La Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos, ofrece una definición de dato personal que versa sobre que la expresión datos personales y abarca cualquier información relativa a un individuo identificado o identificable. Un individuo no se considerará "identificable" si la identificación requiere una cantidad de tiempo y de medios no razonables. En los casos en que el individuo no sea identificable, los datos son denominados anónimos.

[400] AGUAYO ALBASINI, J.L. et al "Sobre la importancia del informe de alta hospitalaria". Revista Cirugía Española, 92(8), 574-576.

1.2.5.1.3. Otros documentos clínicos en el Sistema Nacional de Salud

En la Disposición adicional tercera de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, se establece que el Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición.

Por su similitud terminológica es necesario no confundir el conjunto mínimo de datos del Real Decreto 1093/2010 que aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, con el conjunto mínimo básico de datos del Real Decreto 69/2015 por el que se regula el conjunto mínimo básico de datos al alta hospitalaria, conocido por el acrónimo de CMBD.

El Real Decreto 1093/2010, de 3 de septiembre, aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, norma básica, atendida la diversidad de sistemas y tipos de historias clínicas vigentes en el ámbito de cada comunidad autónoma. Establece el conjunto mínimo de datos que deberán contener una serie de documentos clínicos con el fin de compatibilizar y hacer posible su uso por todos los centros y dispositivos asistenciales que integran el Sistema Nacional de Salud. Asimismo, se garantiza la aplicación de las previsiones de este real decreto en los centros y dispositivos asistenciales que atiendan a los mutualistas y beneficiarios de MUFACE[401], ISFAS[402] y MUGEJU[403].

El artículo 1 del Real Decreto tiene como objeto el establecimiento del conjunto mínimo de datos que deberán contener el listado de documentos clínicos enumerados en el artículo 3 del Real Decreto, cualquiera que sea el soporte, electrónico o papel, en que los mismos se generen. El tipo de dato del conjunto mínimo de datos, vienen detallados en los anexos del Real Decreto y pertenecen a la categoría especial de datos relativos a la salud, se adjunta el Real Decreto ([Anexo AA]).

En base al artículo 3 del Real Decreto, los documentos clínicos para los que se establecen un conjunto mínimo de datos son los siguientes:

- Informe clínico de alta.

[401] MUFACE (2020). Mutualidad General de Funcionarios Civiles del Estado. Año 2020. Disponible en https://www.muface.es/muface_Home/muface_Index.html (31/05/2020).

[402] ISAFAS (2020). Instituto Social de las Fuerzas Armadas. Año 2020. Disponible en https://www.defensa.gob.es/isfas/ (31/01/2021).

[403] MUGEJU (2020). Entidad Gestora del Régimen Especial de Seguridad Social del personal al servicio de la Administración de Justicia. Año 2020. Disponible en https://www.mugeju.es/que-es-mugeju (31/05/2020).

- Informe clínico de consulta externa.
- Informe clínico de urgencias.
- Informe clínico de atención primaria.
- Informe de resultados de pruebas de laboratorio.
- Informe de resultados de pruebas de imagen.
- Informe de cuidados de enfermería.
- Historia clínica resumida.

La historia clínica resumida es un documento electrónico, alimentado y generado de forma automática y actualizado en cada momento, a partir de los datos que los profesionales vayan incluyendo en la historia clínica completa del paciente.

1.2.5.1.4. La historia clínica digital en el Sistema Nacional de Salud

La historia clínica está ampliamente regulada en la Ley 14/2002, de 14 de diciembre. Al concepto de historia clínica hay que añadir el de historia clínica digital.

En cuanto a la historia clínica informatizada el artículo 6, sobre la historia clínica Digital, del Real Decreto-ley 9/2011[404] dice:

> "De acuerdo con lo expresado en el artículo 56 de la Ley de Cohesión y Calidad del Sistema Nacional de Salud y su desarrollo reglamentario en relación al conjunto mínimo de datos de los informes clínicos del Sistema Nacional de Salud y a los efectos de hacer efectivo tanto al interesado como a los profesionales que participan en la asistencia, un acceso adecuado a la historia clínica en todo el Sistema Nacional de Salud en los términos previstos por el ordenamiento jurídico, las administraciones sanitarias establecerán de manera generalizada la conexión e intercambio de información con el Sistema de historia clínica Digital del SNS, antes del 1 de enero de 2013".

El Ministerio de Sanidad, Consumo y Política Social define como objetivos generales de la historia cínica digital, garantizar al ciudadano el acceso por vía telemática a los datos de salud, propios o de sus representados, que se encuentren disponibles en formato digital en alguno de los Servicios de Salud que se integran en el SNS, siempre que cumplan los mínimos requisitos de seguridad establecidos para proteger sus propios datos contra la intrusión ilegítima de quienes no hayan sido facultados para acceder. Además, garantizar a los profesionales sanitarios, facultados por cada Servicio de Salud para esta función, el acceso a determinados conjuntos de datos de salud, generados en una Comunidad Autónoma distinta de aquélla desde la que se requiere la información, siempre que el usuario o paciente demande sus servicios profesionales desde un centro sanitario público del SNS. Y, por último, dotar al SNS de un sistema seguro de acceso que

[404] Real Decreto-ley 9/2011, de 19 de agosto, de medidas para la mejora de la calidad y cohesión del sistema nacional de salud, de contribución a la consolidación fiscal, y de elevación del importe máximo de los avales del Estado para 2011.

garantice al ciudadano la confidencialidad de los datos de carácter personal relativos a su salud.[405]

En algunas Comunidades Autónomas han incluido, además, que el ciudadano pueda conocer los accesos realizados a sus informes clínicos en el sistema de historia clínica Digital del Sistema Nacional de Salud y, en su caso, ocultar aquellos informes clínicos que, según su criterio, no deben ser conocidos por profesionales distintos de quienes habitualmente le atienden[406]. Está regulada en lo que respecta a vertiente tecnológica por el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

1.2.5.2. La receta y la receta electrónica

La receta es el documento de carácter sanitario, normalizado y obligatorio mediante el cual se prescriben[407] a los pacientes los medicamentos o productos sanitarios sujetos a prescripción médica, para su dispensación por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas[408].

Los datos de la receta nacen cuando se emiten y están íntimamente relacionados con la historia clínica, incluso pueden nacer de ella, del tratamiento, pero a pesar de esta íntima relación entre un documento y el otro, la receta no forma parte de la historia clínica.

La naturaleza de la receta es temporal, nace cuando se emiten los datos en el documento, receta, y su fin se agota al ser dispensado, pues el farmacéutico utiliza dichos datos para el acto de dispensación. Las recetas se deberán conservar durante un plazo de tres meses. En el caso de las recetas de psicótropos el plazo de conservación es de cinco años. En el caso de las recetas de la Seguridad Social, esta entidad pública también someterá la receta a tratamiento de datos a la hora de financiar el medicamento. Un caso especial es el de las recetas para la dispensación de estupefacientes.

La normativa que regula la receta tiene un ámbito general que acoge a todo el sistema sanitario español, tanto al sector público como al privado, tal como aparece en el artículo 79 de Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

[405] MS. MINISTERIO DE SANIDAD (2020) "Historia clínica Digital del Sistema Nacional de Salud". p web del Ministerio de Sanidad. Disponible en https://www.mscbs.gob.es/ciudadanos/ portada/ preguntas_ frecuentes.htm (30/01/2021)

[406] CONSEJERÍA DE SANIDAD. MADRID (2020) "historia clínica Digital del Sistema Nacional de Salud". Disponible en https://www.comunidad.madrid/servicios/ salud/historia-clinica-digital-sistema-nacional-salud (31/05/2020).

[407] La RAE define por prescribir: Mandar u ordenar, el médico, que un paciente se tome un medicamento o siga un determinado tratamiento.

[408] Artículo 1 del Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.

En cuanto a la receta electrónica, esta está implantada en el sector público y en el sector privado. Sin embargo, la receta electrónica del SNS viene regulada por el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, concretamente en su capítulo IV "La receta médica electrónica oficial del Sistema Nacional de Salud".

1.2.5.2.1. Régimen ordinario

1.2.5.2.1.1. La receta médica (Anexo BB)

La primera definición de receta médica aparece en el año 1984 en el Real Decreto 1910/1984, de 29 de octubre, receta médica, norma derogada. Definía la receta médica como el documento normalizado por el cual los facultativos médicos legalmente capacitados prescriben u ordenan o mandan la medicación al paciente para su dispensación por las farmacias. El artículo 7 establecía los datos que debía constar en la recetar. Su importancia fue principal, más si se tiene en cuenta que como norma general, los medicamentos sólo serán dispensados con receta de la Ley 25/1990, de 20 de diciembre, del Medicamento, ya derogada.

La receta médica es el documento de carácter sanitario, normalizado y obligatorio mediante el cual los médicos, odontólogos o podólogos, legalmente facultados para ello, y en el ámbito de sus competencias respectivas, prescriben a los pacientes los medicamentos o productos sanitarios sujetos a prescripción médica, para su dispensación por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas o, conforme a lo previsto en la legislación vigente, en otros establecimientos sanitarios, unidades asistenciales o servicios farmacéuticos de estructuras de atención primaria, debidamente autorizados para la dispensación de medicamentos[409]). A la receta médica hay que añadir la receta dispensada por enfermería, que se verá en el capítulo 1.2.5.2.1.2 del Título III, bajo el epígrafe la prescripción de enfermería.

La receta, pública o privada, llevará datos inexcusables para su validez legal así pues constarán los datos relativos al paciente, datos relativos al medicamento, datos del prescriptor y otros datos, artículo 3 del Real Decreto 1718/2010, de 17 de diciembre. De esta forma el Real Decreto 1718/2010 establece que tanto en el sector público como en el privado las recetas pueden emitirse en formato papel, manuscritas manualmente o informatizadas e impresas, o utilizando el soporte electrónico, en cualquier de los casos, el paciente deberá recibir la "hoja de información" en la cual deberá constar la todo lo necesario para hacer posible y facilitar el uso adecuado y correcto del producto.

El artículo 3 del RD 1718/2010, indica los datos que deberán constar en la receta y que estos deberán ser escritos por el propio prescriptor. Los datos que deberá incluir son datos del paciente, datos del medicamento, datos del prescriptor y así como otros datos.

Los datos del paciente que deberán constar en la receta son el nombre, los dos apellidos y el año de nacimiento. En las recetas médicas de naturaleza pública constará el código

[409] Real Decreto 1718/2010, de 17 de diciembre.

de identificación personal del paciente el cual está recogido en su tarjeta sanitaria individual y asignado por su administración pública.

En el caso de ciudadanos extranjeros que no dispongan de la tarjeta sanitaria del sistema nacional de salud, se pondrá el código de su tarjeta sanitaria europea o su certificado provisional sustitutorio (CPS). Si no tuviera ni uno ni el otro, se hará constar el número de pasaporte para extranjeros de países no comunitarios. En todo caso se deberá consignar, asimismo, el régimen de pertenencia de prestación pública del paciente.

En el caso de que la receta fuera expedida por un profesional de la medicina no pública, en casi todos los casos sería privada, se hará constar el número de DNI o NIE del paciente, pero en el caso de que el paciente no disponga de ningún de estos documentos, si fuera menor de edad se hará constar el número de documento de identificación oficial de alguno de sus padres o tutores y si la persona es mayor el número de pasaporte para ciudadanos extranjeros.

El artículo 3 del RD 1718/2010, indica los datos del medicamento que deben constar en la receta. Así se podrá el nombre del principio/s activo/s o del medicamento, junto con la dosificación y forma farmacéutica y, cuando sea el caso, el destinatario, es decir, lactantes, niños o adultos. Será imprescindible incorporar la vía o forma de administración. También aparecerá el número de unidades por envase o contenido de este en peso o volumen, es decir, el formato y el número de envases o número de unidades del medicamento.

La receta constará de la posología o régimen de administración, es decir, el número de unidades de administración por toma, frecuencia de las tomas bien por día, semana o mes y la duración total del tratamiento.

El formato y el número de envases, en las recetas médicas emitidas en soporte electrónico, sólo serán obligatorio incluirlas por el prescriptor cuando el sistema electrónico no los genere de forma automática.

El artículo 3 del RD 1718/2010, indica que deberán constar los datos del prescriptor, tales como su nombre y dos apellidos, población y dirección donde ejerza, además constará siempre el número de colegiado o en el caso del Sistema Nacional de Salud, el código de identificación asignado por la administración competente y, en su caso, la especialidad del profesional. En las recetas médicas de la red sanitaria militar de las Fuerzas Armadas, en lugar del número de colegiado podrá ser sustituido por el número de tarjeta militar de Identidad del facultativo.

La firma será rubricada personalmente una vez cumplimentados los datos descritos y será firma electrónica en las recetas electrónicas, conforme con los criterios establecidos por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

En las recetas del Sistema Nacional de Salud, los datos del prescriptor se podrán consignar de forma que se garantice la identificación del prescriptor y se permita la

mecanización de dichos datos por los servicios de salud y las mutualidades de funcionarios.

El artículo 3.2.d) del RD 1718/2010, en otros datos, cita:

1º. "La fecha de prescripción (día, mes, año): fecha del día en el que se cumplimenta la receta.
2º. La fecha prevista de dispensación (día, mes, año): fecha a partir de la cual corresponde dispensar la receta, en el caso de dispensaciones sucesivas de tratamientos crónicos o medicamentos de dispensación renovable.
3º. N.º de orden: número que indica el orden de dispensación de la receta, en el caso de dispensaciones sucesivas de tratamientos crónicos o medicamentos de dispensación renovable."

Los datos referidos en los epígrafes 2º y 3º se inscribirán en las recetas médicas en soporte papel, tanto públicas como privadas.

Si el medicamento requiere visado deberá ser consignado por la administración sanitaria de acuerdo con el Real Decreto 618/2007. Entendiendo que requieren visado los medicamentos para tratamientos que están autorizados en medio hospitalario; los medicamentos que se utilicen en el tratamiento de enfermedades que deban ser diagnosticadas en medio hospitalario o en establecimientos que dispongan de medios de diagnóstico adecuados; los medicamentos en pacientes ambulatorios que puedan producir reacciones adversas muy graves, lo cual requiere la prescripción por un especialista y una vigilancia especial durante el tratamiento. También se incluyen en este grupo de medicamentos aquellos que por decisión debidamente publicada de la AEMPS tengan reservas singulares, por seguridad o de limitación para determinados grupos de población de riesgo. Por último, también se incluyen los medicamentos para los que se financien algunas de sus indicaciones terapéuticas o que se aplique una aportación reducida en función del tipo de paciente, tal como consta en el Real Decreto 1348/2003.

En caso de recetas electrónicas, el visado se realizará en la forma prevista, artículo 8.7 del RD Real Decreto 1718/2010.

En las recetas médicas en soporte papel y en la hoja de información al paciente para el caso de receta electrónica se incluirá una cláusula que informe al paciente en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. En este caso, a fecha de hoy se entiende que se será de acuerdo a la Ley Orgánica 3/2018.

Documentos similares a las recetas médicas también los pueden realizar otros profesionales. La indicación y autorización de dispensación de medicamentos y productos sanitarios de uso humano por parte de las enfermeras y enfermeros previamente acreditados sólo se podrá realizar mediante orden de dispensación y en las

condiciones recogidas en el párrafo c) del artículo 1 del Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación[410].

El documento de la receta del Sistema Nacional de Salud está íntimamente vinculado al de la tarjeta sanitaria única, así lo determina el artículo 5.2 de Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación al decir que, para la prescripción de recetas médicas oficiales del Sistema Nacional de Salud, el prescriptor recabará del paciente la tarjeta sanitaria individual pudiendo verificar, en caso necesario, su identidad y correspondencia con lo indicado en dicha tarjeta.

Las recetas oficiales del Sistema Nacional de Salud se adaptarán a los criterios básicos de diferenciación de acuerdo con la expresión de las siglas o del código de clasificación en la base de datos de tarjeta sanitaria individual, que figurarán impresos alfanuméricamente o codificado en la parte superior derecha de las recetas, que determina la aportación del usuario en virtud del artículo 5.1 del Real Decreto 1718/2010.

La receta es un documento en el cual deberán constar los datos identificativos de la persona sujeto de la receta, así como los datos que identifiquen a su tarjeta sanitaria Individual y al profesional de la salud que la prescribe.

1.2.5.2.1.2. La prescripción de enfermería (Anexo CC)

La Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios introdujo en nuestro ordenamiento jurídico dos novedades de máxima relevancia incorporando a los podólogos, junto a los médicos y odontólogos, como profesionales sanitarios facultados para recetar, en el ámbito de sus competencias, medicamentos sujetos a prescripción médica. Al mismo tiempo, contemplaba la participación de los enfermeros, por medio de la orden de dispensación, en el uso, indicación y autorización de dispensación de determinados medicamentos y productos sanitarios.

La Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios ha sido sustituida por el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

La prescripción por parte de los profesionales de enfermería se describe y detalla por primera vez en el ordenamiento jurídico español en Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, tras su modificación en el año 2015 por el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el

[410] Real Decreto 1302/2018, de 22 de octubre, por el que se modifica el Real Decreto 954/2015, de 23 de octubre, por el que se regula la indicación, uso y autorización de dispensación de medicamentos y productos sanitarios de uso humano por parte de los enfermeros, que modifica al Artículo 5. Real Decreto 954/2015, de 23 de octubre, por el que se regula la indicación, uso y autorización de dispensación de medicamentos y productos sanitarios de uso humano por parte de los enfermeros.

texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

La orden de dispensación, a la que se refiere el artículo 79 del texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios aprobado por el Real Decreto Legislativo 1/2015, de 24 de julio, es el documento de carácter sanitario, normalizado y obligatorio mediante el cual los profesionales enfermeros podrán prescribir. Todo ello, en el ámbito de sus competencias, y una vez hayan sido facultados individualmente mediante la correspondiente acreditación.

Esta norma[411] es la que indica o autoriza, en las condiciones y con los requisitos que reglamentariamente se establezcan, la dispensación de medicamentos, sujetos o no a prescripción médica, y productos sanitarios por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas o, conforme a lo previsto en la legislación vigente, en otros establecimientos sanitarios, unidades asistenciales o servicios farmacéuticos de estructuras de atención primaria, debidamente autorizados para la dispensación de medicamentos.

El Real Decreto 954/2015, de 23 de octubre, por el que se regula la indicación, uso y autorización de dispensación de medicamentos y productos sanitarios de uso humano por parte de los enfermeros, es modificado por el Real Decreto 1302/2018, de 22 de octubre, por el que se regula la indicación, uso y autorización de dispensación de medicamentos y productos sanitarios de uso humano por parte de los enfermeros.

1.2.5.2.1.3. La receta electrónica del Sistema Nacional de Salud (Anexo DD)

Dentro del Sistema Nacional de Salud, la receta médica electrónica es una modalidad de servicio digital de apoyo a la prescripción dentro de la asistencia sanitaria que permite al facultativo emitir y transmitir prescripciones por medios electrónicos, basados en las tecnologías de la información y comunicaciones, que posteriormente pueden ser objeto de dispensación.

Las administraciones sanitarias en su ámbito de competencia adoptan las medidas precisas para que el aplicativo de la receta electrónica esté implantado y sea interoperable en todo el Sistema Nacional de Salud, desde antes del 1 de enero de 2013, artículo 7 del Real Decreto-ley 9/2011.

La Ley 16/2003, de 28 de mayo, de cohesión y calidad del SNS introduce el término receta electrónica en sus artículos 33 y 54. Esta ley no alcanza a definir la receta electrónica, pero impulsa su implantación.

Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, tan solo hace una breve y escueta referencia la receta electrónica cuando en su artículo 79 dice "La receta médica en soporte papel o electrónico". La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales deroga

[411] Real Decreto 1718/2010, de 17 de diciembre.

concretamente el artículo 79.8 que decía: "No será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico".

La receta electrónica viene regulada por el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, concretamente en su capítulo IV "La receta médica electrónica oficial del Sistema Nacional de Salud". Este tipo de recetas deberán atenerse a los criterios generales sobre receta médica del artículo 6 del Real Decreto 1718/2010, de 17 de diciembre y por descontado a las directrices del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018.

Además de los datos habituales en las recetas en soporte papel este tipo de receta electrónica incluye más datos o códigos, especificados en el artículo 8 del Real Decreto 1718/2010, estos son:

- A fin de garantizar la interoperabilidad entre los diferentes servicios de salud, las recetas médicas electrónicas de cada una de las Administraciones sanitarias deberán necesariamente incorporar el código identificador unívoco de usuarios del Sistema Nacional de Salud y, con carácter exclusivo, el código de identificación del medicamento o del producto sanitario y del resto de parámetros de definición del tratamiento prescrito, que figuren en el nomenclátor oficial de productos farmacéuticos del Sistema Nacional de Salud.
- El sistema de receta médica electrónica de cada una de las administraciones sanitarias del Sistema Nacional de Salud posibilitará la identificación del régimen de pertenencia del paciente, a efectos de cobro de la aportación que en cada caso corresponda, y la realización de la facturación de las oficinas de farmacia a la correspondiente administración sanitaria por medios telemáticos, con las necesarias medidas de seguridad y control que garanticen su correspondencia con las dispensaciones realizadas.
- Por las autoridades sanitarias competentes se determinarán los datos necesarios a los que podrán acceder los farmacéuticos para la facturación de la receta médica electrónica y el desarrollo de programas de calidad de la prestación farmacéutica[412]. En cualquier caso, se facilitará el acceso de los farmacéuticos que posibilite el desarrollo de las funciones contempladas en el artículo 84.1 de la Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios, en las condiciones que se establezcan por las autoridades sanitarias competentes.
- Las administraciones sanitarias públicas son las responsables de la gestión de los sistemas de receta electrónica, por lo que garantizarán la custodia de las bases de datos de prescripción y dispensación y establecerán los criterios de autorización y control de acceso a dichas bases de datos. Todo ello sin perjuicio de los criterios generales de acceso que se establecen en este real decreto.

[412] *Vid Inf p. 342,* capítulo 3.2.4., del Título III.

Este nuevo sistema de prescripción introduce a otro agente del sistema dentro del acceso a los datos del paciente, concretamente a los farmacéuticos y empleados de las oficinas de farmacia. A los efectos de regular este nuevo escenario el Real Decreto 1718/2010 dedica el artículo 9, de la dispensación farmacéutica en la receta médica electrónica, y el artículo 15, actuaciones del farmacéutico de oficina de farmacia en la dispensación.

A los efectos de la seguridad de los datos, el Real Decreto 1718/2010 remitía en su artículo 11 "Protección de la confidencialidad de los datos" a la Ley Orgánica 15/1999. En este orden de cosas, la ley de aplicación es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El Real Decreto-ley 16/2012, de 20 de abril, de medidas urgentes para garantizar la sostenibilidad del Sistema Nacional de Salud y mejorar la calidad y seguridad de sus prestaciones, modifica el artículo 85 bis, sistemas de información para apoyo a la prescripción de La Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios. Está regulada en lo que respecta a vertiente tecnológica por el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

1.2.5.2.2. Régimen especial

1.2.5.2.2.1. Las recetas para dispensación de estupefacientes ($^{Anexo\ EE}$)

Los avances en la medicina han tenido un gran impacto en el tratamiento del dolor de los pacientes o en el alivio de este, en el caso de que se trate de un dolor refractario a la medicación habitual o corriente. Los medicamentos o fármacos usados a estos fines son los denominados medicamentos estupefacientes.

La farmacología no tan solo ha mejorado los mecanismos de acción de este tipo de fármacos, sino que avanzado la utilización de nuevas vías de administración. Todo ello, ha permitido que se incremente considerablemente el número de medicamentos y presentaciones disponibles, lo que supone importantes mejoras en el tratamiento farmacológico del dolor.

Sin embargo, todos estos avances en la ciencia no han sido ajenos al incremento del riesgo de uso indebido de este tipo de sustancia y, lo que es peor, su utilización en el tráfico ilícito de sustancias estupefacientes. Esta situación de riesgo ha llevado a las autoridades a la necesidad de establecer unos requisitos especiales en su prescripción, todo ello encaminado a garantizar la disponibilidad y accesibilidad de los pacientes a los mismos.

Esta normativa permite que España cumpla, además, con los compromisos adquiridos a nivel internacional. En especial los controles derivados de la Ley 17/1967, de 8 de abril, por la que se actualizan las normas vigentes sobre estupefacientes, adaptándolas a lo establecido en el Convenio Único de 1961 sobre Estupefacientes de las Naciones Unidas.

Las recetas especiales para dispensación de estupefacientes vienen reguladas en la Orden PRE/2436/2013, de 26 de diciembre, por la que se modifican los anexos I, II, III y IV del Real Decreto 1675/2012, de 14 de diciembre, por el que se regulan las recetas

oficiales y los requisitos especiales de prescripción y dispensación de estupefacientes para uso humano y veterinario.

La receta Oficial de Estupefacientes (ROE) es el documento imprescindible para la dispensación de medicamentos que contengan sustancias incluidas en la Lista I de la Convención Única de Estupefacientes de 1961, tanto en el ámbito de la asistencia sanitaria pública como en la que se practique con carácter privado.

Este tipo de documento especial cuando se produce dentro del hospital, dispensación intrahospitalaria de estupefacientes, contendrá los siguientes datos: nombre y dos apellidos del facultativo responsable; el número de colegiado o código de identificación asignado por las Administraciones competentes del Sistema Nacional de Salud; los medicamentos estupefacientes que se solicitan; los datos adicionales que sean necesarios para las correspondientes actuaciones de control.

Las recetas oficiales de estupefacientes deberán ir identificadas como receta Oficial de Estupefacientes, con la excepción de aquellas que se emitan en formato electrónico. Las que estén en soporte papel deberán cumplir los requisitos del artículo 5 del Real Decreto 1675/2012, que se exponen en estos puntos:

a) Tener un sistema de numeración que permita una identificación única.
b) Presentarse en talonarios numerados, con 50 recetas igualmente numeradas, cada una de las cuales irá acompañada de una hoja de información al paciente, en la que se recogerá la información del tratamiento necesaria para facilitar el uso adecuado del medicamento estupefaciente; en ambos documentos figurará la misma numeración. Cada talonario deberá incluir además un justificante de recepción de este.
c) La hoja de información al paciente deberá estar diferenciada de la receta propiamente dicha, pudiendo ser separable de la misma mediante copia o trepado.
d) Estas recetas deberán llevar el sello u otro sistema de identificación inequívoco de la institución a través de la cual se haya distribuido el talonario, ya sea la Administración sanitaria o el colegio oficial correspondiente.

Realizada la prescripción, el facultativo firmará y fechará la receta oficial de estupefacientes y la hoja de información al paciente.

El Real Decreto 1675/2012 distingue entre las recetas de estupefacientes emitidas en el sector privado, artículo 4 del Real Decreto 1675/2012, de las emitidas en el Sistema Nacional de Salud, Artículo 6 del Real Decreto 1675/2012.

A partir del día 1 de enero de 2019 está disponible, un año más, la aplicación informática desarrollada por la Agencia Española de Medicamentos y Productos Sanitarios para que las oficinas y servicios de farmacia puedan notificar de forma telemática durante el mes de enero, los datos anuales de movimientos de estupefacientes, según se establece en los puntos 4 y 7 del artículo 17 del Real Decreto 1675/2012, de 14 de diciembre, por el que se regulan las recetas oficiales y los requisitos especiales de prescripción y dispensación de estupefacientes para uso humano y veterinario.

Las nuevas tecnologías para estas prescripciones permitirán integrar en un único documento la receta oficial de estupefacientes y la receta médica de utilización en el ámbito de la asistencia sanitaria pública, haciendo posible que para la dispensación en este ámbito se requiera la presentación de un único documento frente a los dos necesarios hasta el momento, artículo 6 del Real Decreto 1675/2012.

A las recetas de régimen especial para estupefacientes, como documento con información especialmente protegida, hay que añadir el del libro de contabilidad de estupefacientes regulado originalmente en el Real Decreto de 8 de julio de 1930, del reglamento provisional sobre la restricción de estupefacientes y actualmente regulado por Real Decreto 1675/2012, de 14 de diciembre, por el que se regulan las recetas oficiales y los requisitos especiales de prescripción y dispensación de estupefacientes para uso humano y veterinario.

1.2.5.3. La tarjeta sanitaria

Las denominadas tarjetas se han generalizado como soportes documentales de identificación, utilizadas en la sociedad de todo el mundo para identificar al portador como sujeto de derechos, en concreto, como sujeto de los derechos que sustenta la firma, organización, institución o empresa que emite la tarjeta[413].

Así pues, observando a la sociedad occidental no es difícil deducir que la tarjeta es un soporte ampliamente implantado. Existen tarjetas como medios de pago, mediante crédito, mediante débito o mediante prepago, como instrumentos que permiten que su propietario o titular realizar el pago de una cosa, bien o servicio mediante la trasferencia de datos relativos a sus fondos o capacidad financiera.

Hay varias modalidades, además de las mencionadas existen las tarjetas de flota, pago de gasolina, y las tarjeas ATM, tarjetas de cajeros automáticos. Este tipo de tarjeta es tal vez la más conocida, su actividad y garantías están reguladas por Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera que traspone el contenido de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n o 1093/2010 y se deroga la Directiva 2007/64/CE.

También existen las tarjetas de transporte público, como medio de pago del transporte público, con diversas modalidades. También existen tarjetas como identificativo de usuario de un servicio como las tarjetas de fidelización de empresas de servicios y entre otros usos está el que hacen las compañías de seguros para identificar al beneficiario de sus pólizas de seguro. En concreto, dentro de las pólizas de seguro que utilizan la tarjeta como documento de soporte están los seguros médicos o los seguros de salud.

[413] MTMAU. Ministerio de transporte, movilidad y agenda urbana. "Elaboración de tarjetas de identificación y control con soporte de firma digital". Disponible en https://www.mitma.gob.es/el-ministerio/buen-gobierno/proteccion-datos-personales/rat/elaboracion-de-tarjetas-de-identificacion-y-control-con-soporte-de-firma-digital (31/01/2021).

La actividad aseguradora o de aseguramiento se compone, de un asegurador, de el objeto de aseguramiento, un derecho, una prima y la actividad prestadora. El aseguramiento puede venir de mano de una entidad privada o pública[414]. En muchos casos, por no decir en todos, las entidades aseguradoras emiten una tarjeta como soporte del derecho del titular de la prima, estas son las tarjetas sanitarias o tarjetas de salud de las entidades aseguradoras.

Estas tarjetas sanitarias suelen tener incorporada una banda magnética o un chip con la información personal del titular del documento, además de distinta información grabada en la superficie de la tarjeta identificable a simple vista. En algunos casos las tarjetas sanitarias vienen con la foto del titular y en otros casos no. El avance de la tecnología posibilita que las tarjetas sanitarias incorporen datos e información relativa a la salud del titular o bien son portadoras de enlaces electrónicos que permiten el acceso a base de datos con datos e información de salud del titular[415].

En este orden de cosas, en este apartado de la Tesis doctoral, se trata la tarjeta sanitara como documento tanto de soporte del derecho del titular como documento portador de datos relativos a la persona, relativos a códigos identificativos de naturaleza sanitaria o que llevan links o códigos electrónicos que permiten conectar a distancia con bases de datos o con almacenamientos digitales que albergan datos relativos a la salud del titular.

Este apartado, en el contexto del estudio de los datos relacionados con la salud una vez estudiada la historia clínica y la receta, obliga a estudiar la tarjeta sanitaria y en especial la tarjeta sanitaria individual del Sistema Nacional de Salud como documento sanitario más común y de uso corriente por los ciudadanos residentes en España.

Muchos de los aspectos relativos a estas tarjetas son aplicables a las tarjetas de sanidad de compañía privadas. Por último, se tratan algunos aspectos particulares de las tarjetas sanitarias del sector privado.

1.2.5.3.1. La tarjeta sanitaria del Sistema de Nacional de Salud (TSI)

La historia clínica, común en todo el sistema sanitario en España, comparte con la tarjeta sanitaria, en el Sistema Nacional de Salud, relevancia en todo lo que hace referencia a los datos personales y de carácter personal en el escenario de la protección del dato. La tarjeta sanitaria siendo un mero instrumento físico se ha convertido en casi un sujeto con esencia propia.

El Ministerio de Sanidad en su página web con fecha de marzo de 2021 publica que “la tarjeta sanitaria Individual (TSI) es el documento, necesario y suficiente, establecido

[414] FREIRE CAMPO, JM. (2007) “Los sistemas de aseguramiento sanitario de riesgos de enfermedad en España”. Extraordinario Foro SESPAS-AJS. 5 (2), 41-59. Disponible en file:///C:/Users/Juan%20J/ Downloads/ Dialnet-LosSistemasDeAseguramientoSanitarioDeRiesgosDeEnfe-2349374.pdf (31/01/2021).

[415] MEDINACELI DÍAZ, K.I. (2016) “El tratamiento de los datos …..”, op.cit; pp 474-477.

para la identificación de cada ciudadano en el acceso y uso de los servicios del Sistema Nacional de Salud (SNS)"[416].

La tarjeta sanitaria es un documento administrativo que acredita el derecho acceso[417] de los ciudadanos a las prestaciones de la Seguridad Social[418] que proporciona el Sistema Nacional de Salud, mediante determinados datos de su titular, artículo 57.1 de la Ley 16/2003, con un formato único y común válido para todo el Sistema Nacional de Salud, artículo 5 del Real Decreto-ley 9/2011, y con suficiente capacidad de adaptación, en su caso, a la normalización que pueda establecerse para el conjunto de las Administraciones públicas y en el seno de la Unión Europea, artículo 57.5 de la Ley 16/2003.

La TSI incluirá, de manera normalizada, los datos básicos de identificación del titular de la tarjeta, del derecho que le asiste en relación con la prestación farmacéutica y del servicio de salud o entidad responsable de la asistencia sanitaria. Los dispositivos que las tarjetas incorporen para almacenar la información básica y las aplicaciones que la traten deberán permitir que la lectura y comprobación de los datos sea técnicamente posible en todo el territorio del Estado y para todas las Administraciones públicas. Para ello, el Ministerio de Sanidad y Consumo, en colaboración con las comunidades autónomas y demás Administraciones públicas competentes, establecerá los requisitos y los estándares necesarios.[419]

Las características específicas, los datos normalizados y la estructura de la banda magnética de la tarjeta sanitaria Individual se adaptarán a las especificaciones que figuran en el Real Decreto 702/2013, de 20 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

La gran importancia del documento denominado tarjeta sanitaria Individual en toda la normativa de protección de datos personales y el riesgo de que a través de estos documentos se puedan vulnerar viene reforzado, más si cabe, por el artículo 54, Red de comunicaciones del Sistema Nacional de Salud, de Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud determina:

> "El Ministerio de Sanidad y Consumo, a través de la utilización preferente de las infraestructuras comunes de comunicaciones y servicios telemáticos de las Administraciones públicas, pondrá a disposición del Sistema Nacional de Salud una red segura de comunicaciones que facilite y dé garantías de protección al intercambio de información exclusivamente sanitaria entre sus integrantes.
>
> La transmisión de la información en esta red estará fundamentada en los requerimientos de certificación electrónica, firma electrónica y cifrado, de acuerdo con la legislación vigente.
>
> A través de dicha red circulará información relativa al código de identificación personal único, las redes de alerta y emergencia sanitaria, el intercambio de información clínica y

[416] MS. Ministerio de Sanidad (2010). "Interoperabilidad plena de las tarjetas sanitarias" Disponible en https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/tic01.htm (31/01/2021).

[417] Real Decreto-ley 7/2018, de 27 de julio, sobre el acceso universal al Sistema Nacional de Salud.

[418] Artículo 42 del Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.

[419] Artículo 57 de la Ley 16/2003, de 28 de mayo de Cohesión y Calidad del Sistema Nacional de Salud.

registros sanitarios, la receta electrónica y la información necesaria para la gestión del Fondo de cohesión sanitaria, así como aquella otra derivada de las necesidades de información sanitaria en el Sistema Nacional de Salud".

Parece que no hay más que añadir, la propia Ley reconoce la necesidad de que el Ministerio de Sanidad y Consumo pondrá a disposición del Sistema Nacional de Salud una red segura de comunicaciones que facilite y dé garantías de protección al intercambio de información exclusivamente sanitaria entre sus integrantes.

Este riesgo deberá ser analizado mediante los oportunos estudios de evaluación del impacto del tratamiento de datos[420], en el uso de las tarjetas sanitarias y convierte este documento en susceptible de serle de aplicación lo previsto en el artículo 9 del Reglamento (UE) 2016/679 y además conlleva el cumplimiento y la observación de los principios del artículo 5, sobre principios relativos al tratamiento, artículo 6, sobre licitud del tratamiento, y del artículo 7, de condiciones para el consentimiento. La aplicación del artículo 9 estará en consonancia con el Considerando 35 del Reglamento (UE) 2016/679 el cual entiende que se incluye como dato personal relativo a la salud la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria o con ocasión de la prestación de tal asistencia.

1.2.5.3.1.1. Datos básicos comunes de la tarjeta sanitaria individual

La tarjeta tendrá, de manera normalizada, los datos básicos de identificación del titular de la tarjeta, del derecho que le asiste en relación con la prestación farmacéutica y del servicio de salud o entidad responsable de la asistencia sanitaria.

Los dispositivos que las tarjetas incorporen para almacenar la información básica y las aplicaciones que la traten deberán permitir que la lectura y comprobación de los datos sea técnicamente posible en todo el territorio del Estado y para todas las Administraciones públicas, artículo 57.2 de la Ley 16/2003.

Todas las tarjetas sanitarias incorporarán una serie de datos básicos comunes y estarán vinculadas a un *código de identificación personal único* para cada ciudadano en el Sistema Nacional de Salud, independientemente del título por el que accede al derecho a la asistencia sanitaria y de la administración sanitaria emisora.

Con objeto de disponer de datos normalizados de cada persona, en su condición de persona usuaria del Sistema Nacional de Salud, los datos básicos a incluir en el anverso de la tarjeta sanitaria[421] son los que constan a continuación:

a) Identidad institucional de la Comunidad Autónoma o entidad que la emite
b) Los rótulos de "Sistema Nacional de Salud de España" y "tarjeta sanitaria"
c) Código de identificación personal asignado por la administración sanitaria emisora de la tarjeta (CIP-AUT)

[420] *Vid. Supra p. 212* capítulo 3.6., del Título II.

[421] Artículo 3.2 del Real Decreto 702/2013, de 20 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

d) Nombre y apellidos del titular de la tarjeta
e) Código de identificación personal único del Sistema Nacional de Salud (CIP-SNS)
f) Código de identificación de la administración sanitaria emisora de la tarjeta

Las diferentes administraciones sanitarias emisoras, podrán incorporar además a la tarjeta sanitaria el número del documento nacional de identidad de su titular o, en el caso de extranjeros, el número de identidad de extranjeros, el número de la Seguridad Social, la fecha de caducidad de la tarjeta para determinados colectivos o el número de teléfono de atención de urgencias sanitarias, todos ellos en formato normalizado. Igualmente se podrá incluir una fotografía del titular de la tarjeta sanitaria, en los supuestos en los que así lo autorice la ley y pudiendo poner en el ángulo inferior derecho de la tarjeta sanitaria se grabarán, en braille, los caracteres de las iniciales de tarjeta sanitaria Individual (TSI)[422].

1.2.5.3.1.2. Código de identificación personal

El código de identificación personal está reconocido en la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema, concretamente en su artículo 57.3. De tal forma reconoce que, con el objetivo de poder generar el código de identificación personal único, el Ministerio de Sanidad y Consumo desarrollará una base de datos que recoja la información básica de asegurados del Sistema Nacional de Salud, de tal manera que los servicios de salud dispongan de un servicio de intercambio de información sobre la población protegida, mantenido y actualizado por los propios integrantes del sistema. Este servicio de intercambio permitirá la depuración de titulares de tarjetas.

El Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual regula en su artículo 4 el Código de identificación personal del Sistema Nacional de Salud, un elemento crítico para la identificación de las personas en un entorno sanitario o dentro del sector de la salud.

La asignación del código de identificación personal, artículo 57.3 de la Ley 16/2003, del Sistema Nacional de Salud se realizará en el momento de inclusión de los datos relativos a cada ciudadano en la base de datos de población protegida por el Sistema Nacional de Salud, desarrollada por el Ministerio de Sanidad y Consumo, y actuará como clave de vinculación de los diferentes códigos de identificación personal autonómicos que cada persona pueda tener asignado a lo largo de su vida.

La importancia de este código de identificación personal del Sistema Nacional de Salud es intemporal dado que tendrá carácter irrepetible y será único a lo largo de la vida de

[422] Artículo 5.3 y 5.4 del Real Decreto 702/2013, de 20 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

cada persona, independientemente de la Administración pública sanitaria competente en su atención sanitaria en cada momento.

El Real Decreto 183/2004 describe la utilidad del código de identificación, dado que facilitará la búsqueda de la información sanitaria de un paciente que pueda encontrarse dispersa en el Sistema Nacional de Salud, con el fin de que pueda ser localizada y consultada por los profesionales sanitarios, exclusivamente cuando ello redunde en la mejora de la atención sanitaria, con pleno respeto a lo dispuesto en el RGPD y en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, garantizando asimismo la confidencialidad e integridad de la información.

1.2.5.3.1.3. Especificaciones técnicas de la tarjeta sanitaria Individual (Anexo FF)

Las especificaciones técnicas de la tarjeta sanitaria Individual vienen recogidas en el Real Decreto 702/2013, de 20 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual, a lo que hay que añadir el código de clasificación para la aportación del usuario, artículo 5 del Real Decreto 1718/2010.

El Real Decreto, en el anexo, consta la siguiente descripción:

A) Anverso
   1. Ángulo superior izquierdo

      Imagen institucional de la administración sanitaria emisora o fotografía del titular de la tarjeta sanitaria.
   2. Franja superior o universal
      1º. línea (a la derecha): SISTEMA NACIONAL DE SALUD DE ESPAÑA (Arial Narrow, 9 pt, negrita). Rótulo.
      2º. línea (a la derecha): tarjeta sanitaria (TNRoman, 10 pt, negrita). Rótulo.
   3. Franja media

      Entre la segunda línea de la franja superior y la primera línea de la franja inferior se incluirá la imagen institucional de la administración sanitaria emisora de la tarjeta en el caso que en el ángulo superior izquierdo se sitúe la fotografía del titular.
   4. Franja inferior
      1ª. línea: BGKX004499816015 (TNRoman, 11 pt, negrita)

      Significa: Código de identificación personal asignado por la administración sanitaria que emite la tarjeta (Dieciséis dígitos (16): dos primeras consonantes de primer y segundo apellido, fecha de nacimiento, sexo (mujer suma 40 al día de nacimiento), Comunidad autónoma o país de nacimiento, dígitos de repetición de secuencia y dígito de control) ([423]) (CIP o CIP-AUT)
      2ª. línea: Adicionales (TNRoman, 9 pt, normal)

      DNI/NIE (98979695R)

[423] AGUILERA GUZMÁN, M. et al. (2002) "Atención primaria en el INSALUD: diecisiete años de experiencia" Subdirección general de Coordinación Administradita. Instituto Nacional de la Salud. Disponible en https://ingesa.sanidad.gob.es/eu /biblioteca Publicaciones/ publicaciones/ internet/docs/ap17.pdf. p 363. (30/04/2021).

Formato DNI: ocho dígitos y letra de control.

Formato NIE: letra inicial, siete dígitos y letra final de control.

Núm. Seguridad Social (58/68752834/56)

Formato Número Seguridad Social: doce dígitos, dos de provincia, ocho de orden y dos de control.

Fecha caducidad (02/16)

Formato Fecha de caducidad: mm/aa.

Teléfono urgencias (999 999 999)

Formato Teléfono: máximo nueve dígitos

3ª. línea: NOMBRE APELLIDO PRIMERO APELLIDO SEGUNDO (TNRoman, 9 pt, negrita)

Hasta 40 caracteres, si tiene más el punto de truncado sería el último carácter. De ser necesarios más caracteres se minorará el tipo de letra respetando en todo caso la inclusión de los datos en una única línea.

4ª. línea: (BBBBBBBBQR648597) (80724000122) (Braille) (Ambos códigos NTRoman, 9 pt, negrita) (si procede)

CIPSNS (Código de Identificación personal del SNS): 16 caracteres alfanuméricos.

CITE (Código administración sanitaria emisora de la tarjeta): once dígitos (según norma UNE- EN 1387:1997) en el siguiente orden:

- 2 dígitos: área de actividad (80)
- 3 dígitos: código país norma ISO 3166 (España 724)
- 5 dígitos: código de la entidad que emite la tarjeta
- 1 dígito de control

5. Ángulo inferior derecho: A instancia de parte, o de oficio en aquellas administraciones sanitarias que así lo prevean en su normativa, se grabarán en Braille los caracteres de las iniciales de tarjeta sanitaria Individual, siguiendo la norma UNE-EN 1332.1:2010, en su parte 5 de marzo de 2006.

B) Reverso:

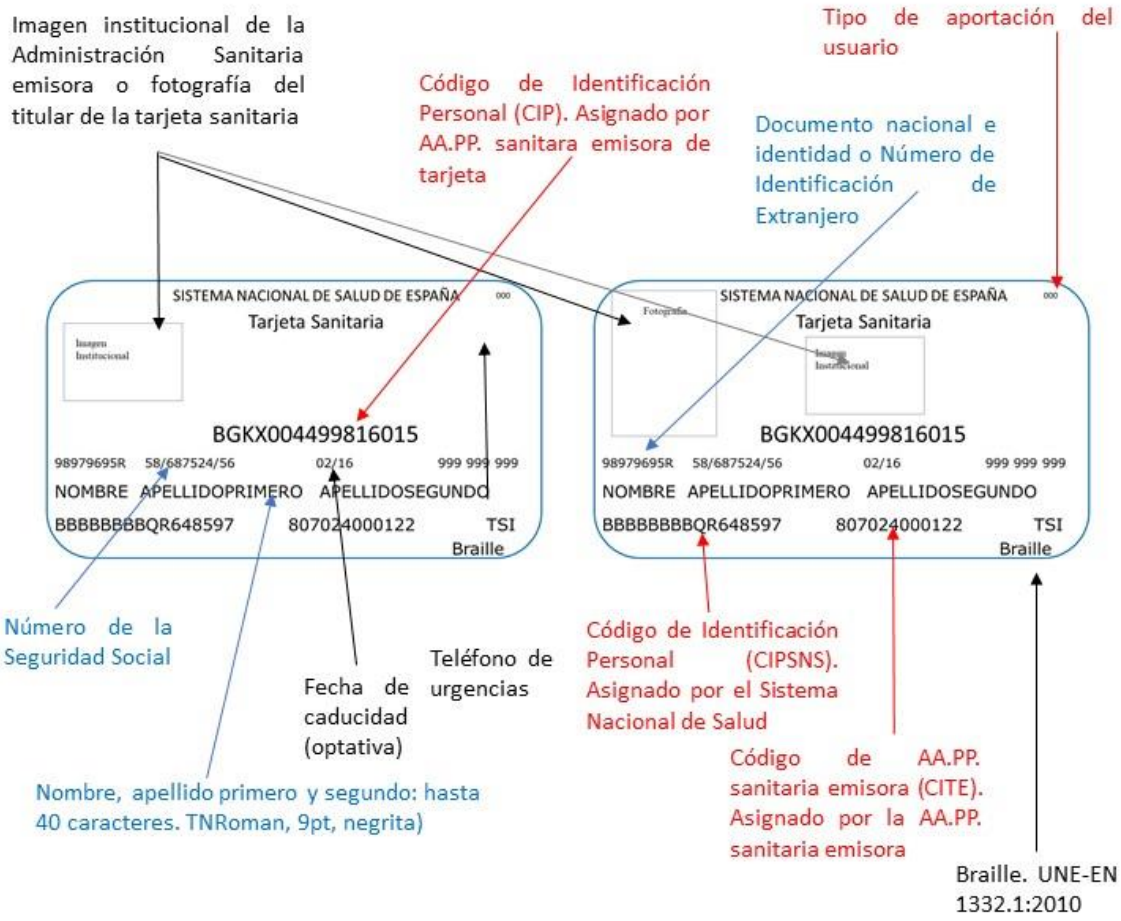
1. Banda magnética con tres pistas:
   a. Pista 1, alfanumérica:
      - CIP-AUT asignado por la administración sanitaria emisora de la tarjeta
      - CIP-SNS único asignado por el Sistema Nacional de Salud
      - Código de la administración sanitaria emisora (dos dígitos, el software de lectura convertirá este código al CITE que figura en el anverso de la tarjeta)
      - Nombre y apellidos del titular
   b. Pista 2, numérica: libre
   c. Pista 3, regrabable
2. Características específicas:
   a. Tamaño de la tarjeta: ID1 siguiendo los estándares ISO 7810 de 1985.
   b. Si la tarjeta incorpora chip su ubicación se atendrá a la norma UNE-EN 1387:1997.
   c. Banda magnética, de alta coercitividad, de lectura-escritura, con tres pistas, norma ISO 7811 de 1985.

Tabla 7. Especificaciones técnicas de la tarjeta sanitaria (elaboración propia)

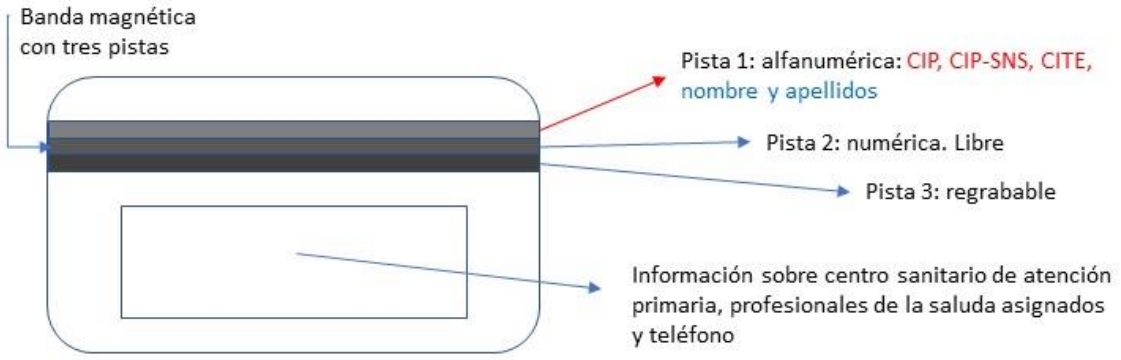
Especificaciones técnicas de la tarjeta sanitaria

Fuente: Real Decreto 702/2013, de 20 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual (Anexo)

Anverso de la tarjeta sanitaria



Dorso de la tarjeta sanitaria



Cuadro de elaboración propia

1.2.5.3.1.4. Base de datos de población protegida del Sistema Nacional de Salud

El Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual en su artículo 6, regula las bases de datos de la Administración pública en cuanto a los datos de los usuario o titulares de las tarjetas sanitarais.

El Departamento de sanidad del Gobierno de España, a través del Instituto de Información Sanitaria, desarrollará una base datos que recoja la información básica de los usuarios del Sistema Nacional de Salud, así como el fichero histórico de las situaciones de aseguramiento y de la adscripción de la persona, en su caso, a diferentes Administraciones sanitarias a lo largo de su vida. El fin de estas bases de datos será el de proceder a la generación del código de identificación personal del Sistema Nacional de Salud.

Esta base de datos actuará como un sistema de intercambio de información entre las Administraciones sanitarias, con el fin de facilitar la gestión de la población protegida, su movilidad y el acceso a los servicios sanitarios. El objeto de la información generada por estas bases de datos será el de la coherencia de los datos de aseguramiento, evitar la adscripción simultánea a distintos servicios de salud y obtener la mayor rentabilidad posible en los cruces de datos entre los ficheros oficiales necesarios para su correcto mantenimiento. Esta base de datos será mantenida por las Administraciones sanitarias emisoras de la tarjeta sanitaria individual, que, a su vez, serán las competentes para la inclusión en aquélla de las personas protegidas en su ámbito territorial siendo las responsables del tratamiento de los datos, actuales e históricos, de su población protegida.

La base de datos incorporará información del sistema de Seguridad Social y del mutualismo administrativo, con el fin de suministrar a las Administraciones sanitarias datos permanentemente actualizados que permitan la correcta gestión de las situaciones de las personas respecto a altas, bajas, cobertura de prestaciones y movilidad de pacientes en la Unión Europea, de acuerdo con los reglamentos comunitarios vigentes en esta materia.

El plan de explotación estadística de la base de datos será acordado por el Consejo Interterritorial del Sistema Nacional de Salud, y la información obtenida se pondrá a disposición de las Administraciones sanitarias. En todo caso, la información que se facilite a estos fines será previamente objeto de disociación, artículo 5.6 del Real Decreto 183/2004.

1.2.5.3.2. Tarjeta sanitaria europea

La tarjeta sanitaria europea, deriva de la aplicación de los Reglamentos europeos relativos a la Seguridad Social. La normativa recogida en estos Reglamentos se centra en los acuerdos entre los sistemas de Seguridad Social y la Directiva 2011/24/UE, no afecta a las prestaciones ya reconocidas en los mencionados Reglamentos. Por lo tanto, los ciudadanos que necesiten asistencia, incluso de urgencia, al encontrarse temporalmente en el extranjero seguirán beneficiándose de la reglamentación existente y recibiendo los cuidados que precisen.

La aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza dentro de la Unión Europea tiene dos fuentes de derecho derivado, la Directiva 2011/24/UE, del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, y los Reglamentos de la Unión sobre la coordinación de los sistemas de Seguridad Social, Reglamento (CE) nº 883/2004 en artículo 11 y artículos 17 a 20, supuesto de aplicación de la tarjeta sanitaria europea.

Si un paciente solicita expresamente que se le aplique un tratamiento en virtud de la Directiva 2011/24/UE, no es aplicable la tarjeta sanitaria europea, los beneficios que se apliquen al reembolso quedarán limitados a los aplicables en virtud de la directiva. Cuando el paciente tenga derecho a asistencia sanitaria transfronteriza en virtud tanto de la Directiva 2011/24/UE como del Reglamento (CE) nº 883/2004 y la aplicación de dicho reglamento sea más ventajosa para el paciente, el Estado miembro de afiliación le señalará este hecho.

Los Reglamentos de coordinación de los sistemas de Seguridad Social Reglamento CEE 1408/71 reemplazado por el Reglamento 883/2004, que entró en vigor en mayo de 2010, facilitan cierto nivel de reciprocidad en la cobertura de la asistencia sanitaria de los ciudadanos del Espacio Económico Europeo. En concreto, se aplican a: los turistas que requieren asistencia sanitaria durante su visita a otro Estado miembro, las personas que viven y trabajan en el extranjero, o, en ciertas circunstancias, aquellos que desean viajar para recibir asistencia sanitaria. El Reglamento cubre también a los pensionistas y las disposiciones de seguridad social, incluyendo la asistencia sanitaria, que se transfieren de un Estado a otro al llegar a la jubilación.

1.2.5.3.3. Las otras tarjetas sanitarias

La tarjeta sanitaria individual del Sistema Nacional de Salud es sin duda el documento que acredita el derecho más utilizado en España. Sin embargo, no hay que olvidar el importante número de tarjetas sanitarias de compañías de seguros de salud privados hay en España.

La sanidad privada ocupa el 28,8% del gasto sanitario total en España, siendo el gasto sanitario en España en el año 2018 el 9% del producto interior bruto. España en 2018 las compañías de seguros de salud tenían 8,5 millones de asegurados, de los cuales aproximadamente 1,8 millones de personas, corresponden al régimen de mutualismo administrativo que acoge a la Mutualidad General de Funcionarios Civiles del Estado, MUFACE, a la Mutualidad General Judicial, MUGEJU, y al Instituto Social de las Fuerzas Armadas, ISFAS.[424]

Todas las características atribuidas a la tarjeta sanitarias del SNS, excepto las exclusivas, todas las reglas de funcionamiento y restricción al tratamiento de sus datos son

[424] IDIS. Fundación Instituto para el Desarrollo e Integración de la Sanidad (2020) "Sanidad privada, aportando valor. Análisis de situación 2019". Madrid. La Fundación Instituto para el Desarrollo e Integración de la Sanidad (IDIS). Disponible en https://www.fundacionidis.com/informes/analisis-de-situacion-de-la-sanidad-privada/sanidad-privada-aportando-valor-analisis-de-situacion-2019 (31/01/2021).

extensibles a las tarjetas sanitarias de las compañías de seguros de salud privadas y a todas las bases de datos que estas compañías puedan utilizar.

1.2.5.4. El Registro de Actividad de Atención Especializada-CMBD

> "El concepto de conjunto mínimo de datos básicos fue formulado por primera vez en 1969 en el contexto de una conferencia sobre sistemas de información sanitarios en los Estados Unidos (Treviño, 1988; Foster y Conrick, 1998). Desde entonces hasta la actualidad el CMBD ha ido evolucionando a nivel internacional".[425]

El Comité Nacional de Estadísticas Vitales y Sanitarias de EEUU desarrolló el Uniform Hospital Discharge Data Set (UHDDS), en 1973, como el conjunto de datos básicos extraídos de la información de las historias clínicas de los pacientes ingresados[426].

En 1981 la Comunidad Económica Europea desarrolló el European Minimum Basic Data Set (MBDS) utilizando el modelo norteamericano como referencia. Junto a la OMS y el Comité Hospitalario de las Comunidades Europeas definen el CMBD al alta hospitalaria como un núcleo de información mínimo y común sobre los episodios de hospitalización. El Consejo de Europa lo incluyó como parte integrante del sistema de información hospitalario[427].

El Consejo Interterritorial del Sistema Nacional de Salud aprobó, en el pleno celebrado el 14 de diciembre de 1987, el Conjunto Mínimo Básico de Datos al Alta Hospitalaria, como instrumento que garantice la uniformidad y suficiencia de la información recogida para cada episodio asistencial en el conjunto del Sistema Nacional de Salud, siguiendo la recomendación del informe "European Minimun Base Data Set" realizada en 1979 por el subgrupo BM3 perteneciente al Comité de Información y Documentación Clínica y Tecnología en la CEE[428]

El Conjunto Mínimo Básico de Datos (CMBD) supone un extracto impersonal de información administrativa y clínica, que debe ser recogida a partir del informe de alta, al que no sustituye en ningún caso y completada, si es necesario, con la historia clínica[429].

El Registro de Actividad de Atención Especializada-CMBD se implanta en 2016 como nuevo modelo de datos del Conjunto Mínimo Básico de Datos de las Altas Hospitalarias extendiendo el registro a otras áreas alternativas a la hospitalización tales como al hospital de día, gabinetes de técnicas y procedimientos de alta complejidad y urgencias,

[425] MARCO CUENCA, G. SALVADOR OLIVAN, J.A. (2018) "Del CMBD al Big Data en salud: un sistema de información hospitalaria para el siglo XXI". Scire Scire: representación y organización del conocimiento, 24 (1), 77-89. pp 78-79.

[426] LÓPEZ GONZÁLEZ, R. (19-21 noviembre de 2008) "CMBD ¿Qué es y para qué nos sirve?" XXI Congreso Nacional de la SEMI. Disponible en https://www.fesemi.org/sites/default/files/ documentos/ ponencias/ XXIX-congreso-semi/Dr.%20Lopez%20GOnzalez.pdf (31/05/2021). P 5.

[427] ROGER, FH. (1981) "The minimum basic data set for hospital statistics in the EEC". Commission of the European Communities. ECSC-EEC-EAEC, Brussels. Luxembourg. pp-2-3.

[428] TEMES, JL. (2002) "Gestión Hospitalaria". Madrid. Ed. McGraw-Hill. pp 188-189.

[429] DECRETO 89/1999, de 10 de junio, por el que se regula el conjunto mínimo básico de datos (CMBD) al alta hospitalaria y cirugía ambulatoria, en la Comunidad de Madrid.

y al sector privado. Su estructura, formato y contenidos, así como las normas para el registro y envío de la información se recogen en el Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención Sanitaria Especializada.

El artículo 5 "Contenido del registro" de Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención sanitaria Especializada, determina que contendrá:

1. Tipo de código de Identificación Personal
2. Código de Identificación Personal
3. Número de historia clínica
4. Fecha de nacimiento
5. Sexo
6. País de nacimiento
7. Código postal del domicilio habitual del paciente
8. Municipio del domicilio habitual del paciente
9. Régimen de financiación
10. Fecha y hora de inicio de la atención
11. Fecha y hora de la orden de ingreso
12. Tipo de contacto
13. Tipo de visita
14. Procedencia
15. Circunstancias de la atención
16. Servicio responsable de la atención
17. Fecha y hora de finalización de la atención
18. Tipo de alta
19. Dispositivo de continuidad asistencial
20. Fecha y hora de intervención
21. Ingreso en Unidad de Cuidados Intensivos
22. Días de estancia en Unidad de Cuidados Intensivos
23. Diagnóstico principal
24. Marcador POA1 del diagnóstico principal
25. Diagnósticos secundarios
26. Marcador POA2 de los diagnósticos secundarios
27. Procedimientos realizados en el centro
28. Procedimientos realizados en otros centros
29. Códigos de morfología de las neoplasias
30. Centro sanitario
31. Comunidad autónoma del centro sanitario

El artículo 6 del Real Decreto 69/2015, establece que la Unidad de registro es, con carácter general, el contacto. La expresión "el contacto" se define como la atención sanitaria prestada bajo la misma modalidad asistencial y de forma ininterrumpida por un proveedor sanitario a un paciente. Los tipos de contacto, en función de la modalidad asistencial, son: Hospitalización; Hospitalización a domicilio; Hospital de día médico; Cirugía ambulatoria; Procedimiento ambulatorio de especial complejidad; y Urgencia.

El artículo 7.2, modelo y soporte de datos, del Real Decreto 69/2015 establece que el registro se implementará en soporte digital y su diseño y estructura permitirán que el intercambio de datos y su explotación pueda realizarse por medios electrónicos.

El CMBD se usa para aplicar el sistema de los GDRs, Grupos Relacionados por el Diagnóstico, básicamente un sistema que permite agrupar a los casos y asignarles un índice de complejidad a cada caso[430].

[430] YETANO LAGUNA, J, LÓPEZ ARBELOA, G (2010) "Manual de descripción de los Grupos Relacionados por el Diagnostico". Oskidetza. Servicio Vaso de Salud. Victoria-Gasteiz. Edición 5ª. pp 5-6.

Capítulo 2. Principios del tratamiento de datos relativos a la salud y los derechos que hace posible la efectividad del derecho a la protección de los datos personales en el sector de la salud

2.1. Los principios de la protección y del tratamiento de datos en la normativa de protección de datos personales en el sector de la salud

2.1.1. Con carácter general

El origen de este principio en el contexto europeo data del Convenio, número 108, del Consejo de Europa de 28 de enero de 1981, para la Protección de personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional de 8 de noviembre de 2001. Concretamente el aparado 45 de la memoria Explicativa del Convenio introduce la definición de datos de carácter personal relativos a la salud y considera que abarca "las informaciones concernientes a la salud pasada, presente y futura física o mental de un individuo, pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido"[431].

En el contexto de España la protección del dato de los pacientes nace de dos fuentes de derecho. Por una parte, de la protección de los datos de carácter personal de cualquier persona y por la otra parte, de la regulación de la información que genera la persona cuando adquiere el rol de paciente, que, si bien las dos normas confluyen en los datos personales relativos a la salud, cada norma actúa en base a principios distintos.

La norma regulatoria de la protección del dato personal, Reglamento (UE) 2016/679, pone su mirada en los derechos fundamentales de las personas, derecho a la intimidad entre otros, por otra parte, la norma regulatoria de la información clínica[432], crea un derecho en base al principio de la autonomía de la persona.

Esta protección de los datos de la persona actúa en dos dimensiones. En primer lugar, cualquier información concerniente a personas físicas identificadas o identificables, Ley Orgánica 3/2018 y el Reglamento (UE) 2016/679. En segundo lugar, la dimensión especial que le da ordenamiento jurídico, la Ley Orgánica 3/2018 lo resuelve entre su artículo 9, el artículo 28.2, y, en especial, en su Disposición adicional decimoséptima sobre Tratamientos de datos de salud.

De tal forma que los datos de las personas están protegidos y tienen una doble protección cuando estos afectan a sus derechos fundamentales o a bienes jurídicos, como la salud.

La regulación de la información del paciente tiene sus antecedentes en la gran importancia que ha tenido el derecho del paciente en los acuerdos internacionales desde la Segunda Guerra Mundial. Tanto la Declaración sobre la promoción de los derechos de los pacientes en Europa, promovida el año 1994 por la Oficina Regional para

[431] BERROCAL LANZAROT, AI (2011) "La protección de datos relativos a la salud y la historia clínica en la normativa española y europea". Revista de la Escuela de Medicina Legal, 18, 12-44. pp 17, 18, 22.

[432] Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Europa de la Organización Mundial de la Salud como otras tantas declaraciones inspiradas en la Declaración Universal de Derechos de Humanos de 1948[433]. El primer instrumento internacional con carácter jurídico vinculante para los países que lo suscriben es el Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina, Convenio sobre los derechos del hombre y la biomedicina, suscrito el día 4 de abril de 1997, el cual entró en vigor en el Reino de España el 1 de enero de 2000.

El derecho a la información en el proceso clínico ha sido atendido por el ordenamiento jurídico desde que en 1986 se promulgó la Ley 14/1986, de 25 de abril, General de Sanidad, que, si bien ha sido ampliamente discutida[434], introdujo nuevos principios en el sistema sanitario español innovando en el principio del respeto a la confidencialidad de la información relacionada con los servicios sanitarios tanto públicos como privados.

La Directiva comunitaria 95/46, de 24 de octubre de 1995, defiende otros dos principios, por una parte, el de la confidencialidad en la información clínica y, por otra parte, el de la intimidad relativa a la información relacionada con su salud, iniciando, a su vez, el marco de excepciones de los derechos de los pacientes en esta materia. Estas excepciones se fundamentan en la presencia de otros intereses generales como los estudios epidemiológicos, las situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos que, cuando estén incluidos en normas de rango de Ley.

El Consejo de Europa, en su Recomendación de 13 de febrero de 1997, relativa a la protección de los datos médicos, después de afirmar que deben recogerse y procesarse con el consentimiento del afectado, indica que la información puede restringirse si así lo dispone una Ley y constituye una medida necesaria por razones de interés general.

[433] OMS (20-30 mayo 1994) "Declaración para la promoción de los derechos humanos en Europa". Oficina regional para Europa. Disponible es https://www.ffis.es/ups/documentacion_ley_3_2009/Declaracion_promocion_derechos_pacientes_en_Europa.pdf (28/02/2021).

[434] La Ley General de Sanidad fue aprobada el 25 de abril de 1986, tan solo cuatro años después el Congreso de los Diputados encargo un análisis del Sistema Sanitario que había creado dicha ley. En las conclusiones del Informe consta: "*Finalmente, y por no alargarme más porque todos ustedes disponen de la estructura y el comentario del informe, quisiera decir que en todos los contactos y reuniones que hemos tenido hemos podido apreciar unos deseos enormes de mejora y una gran esperanza en núcleos profesionales, etcétera, de que se inicien caminos de reforma y de mejora. Hemos podido apreciar también en distintas esferas administrativas que tienen la responsabilidad de administrar esta enorme necesidad social, el sentido de frustración, el sentido de impotencia y, al mismo tiempo, el deseo de luchar contra estas cosas que impiden realmente el funcionamiento armónico, útil y sin rechinamientos excesivos del sistema. Nos ha parecido encontrar en la sociedad, en los estamentos de responsabilidad, en los núcleos profesionales, en todas las áreas privadas que quieren colaborar y trabajar en este campo, en la iniciativa privada, que es insuficiente o pequeña, pero emergente en este momento, en definitiva, en todo el estamento técnico-administrativo, que existe una gran inquietud, que entendemos que supone una gran riqueza colectiva y social. Si se acierta a encauzar esa gran riqueza en un impulso efectivo, creo que se habrá efectuado un servicio muy útil a España*." de la Comparecencia del señor Presidente de la Comisión de Expertos encargada del análisis y evaluación del Sistema Nacional de Salud (Abril Martorell), para informar de las conclusiones de la citada Comisión, creada por resolución de esta Cámara de fecha 13 de febrero de 1990. Solicitada por el Grupo Parlamentario Socialista (número de expediente 219/0002&1). BOE 25 DE SEPTIEMBRE DE 1991.-NÚ. 306.

En este orden de cosas, es de nuevo el valor de la intimidad estrechamente vinculado al de la digitad humana los que se ven protegidos, en este caso junto al del valor de la autonomía de la voluntad como expresión del principio de la libertad de la persona, la cual no se puede ejercer sin información[435].

Así pues, son esos bienes jurídicos los que el ordenamiento jurídico protege y regula mediante la legislación relativa a la información clínica del paciente y lo hace en base al principio de que la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad que deben orientar toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica. A estos principios se les suman los del previo consentimiento de la persona, paciente o usuarios, y del cumplimiento de los deberes, por parte de los profesionales, de información y de documentación clínica y de la reserva debida en relación con estas.

A estos principios, que sustentan los derechos de los pacientes, se añaden otros principios que justifican las obligaciones de estos en materia de datos, de aquí el principio del deber del paciente de facilitar datos sobre su salud cuando se reclame la atención o asistencia de esta. De tal forma, los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria, artículo 2.5 de la Ley 41/2002.

2.1.2. En el marco del Reglamento General de Protección de datos

El capítulo 3.1. del Título I, destaca que el primer principio que emana del Reglamento 2016/679 es el principio de proactividad, también llamado de responsabilidad proactiva, estando asignada al responsable del tratamiento[436].

Otro principio que emana del Reglamento 2016/679 es el de la protección pasiva del dato. Este un principio no explicitado pero que emana del Reglamento y que establece que todos los datos personales están protegidos, es decir, no permite ningún tratamiento de ningún dato excepto el tratamiento que se somete al artículo 6, prohibiendo el artículo 9 el tratamiento de los datos relativos a la salud, entre otros.

El principio de minimización de los datos personales que aparece en el Reglamento (UE) 2016/679 mencionado en los artículos 5, 25, 47 y 89 y en el Considerando 156. Este principio goza de una especial importancia en el sector sanitario, de tal forma que no es posible hacer acopio ni tratar datos relativos a la salud de las personas por si pudiera ser necesario en un futuro y no hay ninguna excepción en este principio que emane del artículo 9.

[435] STC 37/2011 de 28 de marzo de 2011 (Sala Segunda), FD 5º.

[436] AEPD (2019) "Guía del Reglamento General de Protección de Datos. Para responsables del tratamiento". Guía de protección de datos UE. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf (31/01/2021). p 3.

Por otra parte, también es cierto que en el apartado 2 del mismo artículo 9, excepciona determinados supuestos de la prohibición establecida sobre el tratamiento de los datos relaticos a la salud, pero en ningún caso a la expresión se aplica a este principio sino tal solo al requisito del consentimiento.

Los principios que aparecen en el Capítulo II del Reglamento (UE) y en el Título II de la Ley Orgánica 3/2018 y que la AEPD expone en su documento de diciembre de 2019, en cuanto se refiere a sector sanitario cabe decir[437]:

A) La licitud, la lealtad y la transparencia, con relación al interesado: el tratamiento de datos en el sector sanitario no presenta diferencias o nuevas exigencias en relación al tratamiento de los datos de las personas con carácter general.

B) La limitación de la finalidad: los datos no serán tratados con fines distintos por los que fueron recogidos. El tratamiento de datos en el sector sanitario presenta diferencias y nuevas exigencias, que están reflejadas en las excepciones que plantea el artículo 9.2 del Reglamento (UE) 2016/7679 en el cual la finalidad de la salud de la persona titular se ve superada cuando está en juego el interés público esencial, artículo 9.2.g) y artículo 9.2.j) o la salud pública, artículo 9.2.i). Los datos se recogerán con fines determinados, explícitos y legítimos, y no serán usados posteriormente para finalidades incompatibles con dichos fines. Si la persona consiente en la utilización de sus datos para fines de una concreta investigación científica, por ejemplo, cáncer de colón, se podrán utilizar para otras investigaciones oncológicas. Esta segunda utilización no se considera incompatible, según AEPD en su documento de diciembre de 2019.

C) La minimización de datos: el tratamiento de datos en el sector sanitario no presenta diferencias o nuevas exigencias en relación al tratamiento de los datos de las personas con carácter general. Sólo se van a utilizar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; es decir, que solo van a recoger, en general, los datos mínimos necesarios para prestar la mejor asistencia sanitaria. Aunque esta información puede ser amplia dada la variedad de factores que pueden afectar a la salud como pueden ser la comida, bebida, antecedentes familiares, hábitos, entre otros muchos, según AEPD en su documento de diciembre de 2019. “Una interpretación sistemática del RGPD, cabe inferir que el principio de minimización impide una acumulación masiva e indiscriminada de datos de salud sean o no pertinentes para el fin perseguido”[438].

D) La exactitud de los datos: el tratamiento de datos en el sector sanitario no presenta diferencias o nuevas exigencias en relación al tratamiento de los datos de las personas con carácter general. Si bien es cierto, que la propia naturaleza y finalidad de los datos relativos a la salud de una persona conllevaría un mayor rigor

[437] AEPD (2019) “Guía para pacientes y usuarios de la sanidad”. Diciembre 2019. Disposición en https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf (28/02/2021).
[438] BELTRÁN AGUIRRE, JL (2018) “Reglamento general …..”. op.cit; p 74-76, p 85.

en la aplicación de este principio. En las historias clínicas, es el profesional sanitario el que determina qué datos se pueden suprimir o rectificar, según AEPD en su documento de diciembre de 2019.

E) La confidencialidad: el deber de confidencialidad es un principio nombrado como tal en la Ley Orgánica 3/2018, artículo 6, e incluido dentro de los principios relativos al tratamiento en el Reglamento (UE) 2016/679, artículo 5. Este principio viene reforzado por la exigencia de secreto profesional del artículo 9.2.i) y 9.3 del Reglamento (UE) 2016/679, cuando se levanta la prohibición de tratamiento de los datos con un tratamiento especialmente protegido y se aplica la excepción. Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de dichos datos, incluida la protección contra el tratamiento y acceso no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas, según AEPD en su documento de diciembre de 2019.

F) Licitud de tratamiento: el tratamiento de datos en el sector sanitario no presenta diferencias o nuevas exigencias en relación al tratamiento de los datos de las personas con carácter general. En base al TJUE, que entiende por licitud del tratamiento cuando este es proporcional y necesario[439], se entiende que a la exigencia de la licitud del artículo 6 se aplica la necesidad de su tratamiento en base a la naturaleza del dato en el sector sanitario y que la proporcionalidad se aplicará en relación al riesgo y vulnerabilidad de la persona en relación a los datos sobre su salud o los vinculados con el proceso asistencial.

G) El consentimiento: este principio es el único que se excepciona con la aplicación del artículo 9.2. La prohibición del tratamiento de los datos relativos a la salud, que en base al Considerando 35 se incluyen los de la persona en el sector sanitario, se excepciona en la exigencia del consentimiento en los supuestos del artículo 9.2. También el levantamiento o exención de este principio sufre excepciones, estas excepciones son las que la legislación de cada país impone a la limitación del consentimiento de la persona, es decir, una persona no puede decidir que sus datos se hagan públicos siempre y en todos los casos, sino solo en los que la ley no lo prohíbe o limita.

H) El consentimiento del menor: se aplica el mismo criterio que en el apartado anterior.

I) Las categorías especiales de datos: a esta categoría especial de datos personales se conocen como datos sensibles, se prevé para ellos una seguridad reforzada[440].

J) El tratamiento de los datos de naturaleza penal: el tratamiento de datos en el sector sanitario no presenta diferencias o nuevas exigencias en relación al tratamiento de los datos de las personas con carácter general.

[439] STJUE de 16 de diciembre de 2008 (Gran sala) (asunto C-524/06) apartado 52.
[440] SAN 4845/2018 de 20 de diciembre (Sala de lo Contencioso), FD 6º.

K) El tratamiento de los datos sin identificación: si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

L) Otros principios: el Reglamento (UE) 2016/679 añade una serie de principios distintos de los mencionados con anterioridad de esta forma se refiere y que en relación a los datos relativos a la salud o a la persona en el sector sanitario, se refiere a:

a. principio de periodos de conservación limitados; este principio se trata en el capítulo 3.2.3.1 del Título III. Los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales. Los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. La historia clínica debe conservarse durante todo el tiempo que se va a prestar asistencia sanitaria; para facilitarlo a los órganos judiciales, si lo solicitan; para efectuar estudios epidemiológicos, docencia e investigación. En este último supuesto, podrían pseudonimizarse, es decir, separar los datos identificativos del paciente de los de salud, aunque puedan volver a asociarse si es necesario, según la AEPD en su documento de diciembre de 2019.

b. principio de la calidad de los datos: en el sector de la salud este principio tiene una extremada importancia y está en conexión tanto con el principio de la protección de los datos desde el diseño como con el principio de la exactitud de los datos.

c. principio de la protección de los datos desde el diseño y por defecto: este principio que garantiza en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona titular, a un número indeterminado de personas físicas. En cuanto a los datos relativos a la salud y al sector sanitario, tienen una especial relevancia por el alto contenido de confidencialidad inherente que conlleva, de esta forma el Reglamento (UE) en su artículo 25.1 señala que se tendrán en cuenta en el diseño “los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas” de los datos a tratar. Cabe recordar que el artículo 25 del Reglamento (UE) 2016/679 aparece el criterio general sobre este principio:

> el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en

el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

El artículo 25 en su apartado 2, señala al responsable del tratamiento como la persona que deberá tener en cuenta este principio garantizando que solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

El mismo apartado entiende que este principio está en íntima conexión con el principio de minimización y al de su conservación, así como con la necesidad de limitar de la extensión de su tratamiento a lo necesario e indispensable y al contexto de su accesibilidad.

d. principio de las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes, artículo 4, Normas corporativas vinculantes, Reglamento (EU) 2016/679).

Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable, y en especial a los datos recogidos en el artículo 9 del Reglamento (UE) 2016/679. El Reglamento no afecta al tratamiento de la información anónima, inclusive con fines estadísticos o de investigación, tal como consta en el Considerando 26 del Reglamento (UE) 2016/679.

2.2. Los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de los datos personales en el sector de la salud

El capítulo 4.1, del Título I trata los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de los datos personales con carácter general. Este capítulo 2.2. del Título III tratará los mismos derechos, pero aplicados al tratamiento de los datos relativos a la salud o al sector sanitario en el cual se ubica la persona y sus datos.

Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario. El Reglamento (UE) 2016/679, manteniendo los tradicionales derechos de acceso, rectificación, cancelación y oposición, suman otros cuatro nuevos derechos, el derecho al olvido, el de portabilidad de los datos, el derecho a la limitación del tratamiento y el derecho a no ser objeto de decisiones individualizadas.

El Reglamento (UE) en su artículo 1 protege el derecho a la protección de los datos personales personas físicas, como derecho fundamental que reconoce que es. Este artículo 1 está conectado con el artículo 6, el que legitima cualquier tratamiento de datos y con el artículo 9, el que prohíbe el tratamiento de datos especiales como son los relativos a la salud de las personas o a los datos de las personas que operan en el sector sanitario, Considerando 35.

Reglamento (UE) 2016/679 reconoce una serie de derechos en relación a los datos personales y que son perfectamente trasladables al supuesto de los datos relativos a la salud, aunque con algunos matices.

El capítulo 4.1. del Título I, sobre "Los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de los datos personales" analiza el documento de la AEPD publicado el día 20 de julio de 2019 con el título "Ejerce tus derechos"[441] en el cual explica que la normativa de protección de datos permite que la persona pueda ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión o "derecho al olvido", limitación del tratamiento, portabilidad y de no ser objeto de decisiones automatizadas individualizadas.

En relación al documento "Ejerce tus derechos" y en conjunción con el documento de la AEPD de noviembre de 2019 denominado "Guía para pacientes y usuarios de la Sanidad" [442], cabe especificar que los derechos de la persona en relación a sus datos relativos a su salud o a sus relaciones con el sector sanitario se rigen por estas características:

1. Su ejercicio es gratuito y obligado salvo en caso de solicitudes "manifiestamente infundadas o excesivas especialmente debido a su carácter repetitivo", en base al documento de la AEPD de diciembre de 2019.
2. Derecho a ser informado:
    a. De la identidad y nombre del responsable del tratamiento de sus datos, pudiendo ser el médico privado, profesional sanitario de la compañía de seguro médico suscrito, hospital público o privado, o Servicio de Salud de la Comunidad Autónoma.
    b. De los datos del delegado de protección de datos, excepto las consultas privadas de un profesional sanitario.
    c. De los fines del tratamiento de sus datos y base jurídica del mismo.
    d. De los destinatarios se sus datos personales.
    e. De la intención por parte del responsable de transferir sus datos.
    f. Del plazo de conservación de los datos.
    g. Por el responsable sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio.
3. Derecho a solicitar del responsable, acceso a los datos.
4. Derecho a retirar su consentimiento en cualquier momento, sin que ello afecta a la licitud del tratamiento basado en el consentimiento previo a su retirada.
5. Derecho a presentar una reclamación ante una autoridad de control y derecho a presentar dicha reclamación ante el DPO.

[441] AEPD (2019) "Ejerce tus derechos". 20 de Julio de 2019. Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos (31/01/2021).

[442] AEPD (2019) "Guía para pacientes y usuarios de la sanidad". Diciembre 2019. Disposición en https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf (28/02/2021).

6. Derecho a ser informado de la existencia y uso de decisiones automatizadas, es decir, tomadas mediante procesos informáticos sin intervención humana, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o le afecten significativamente de modo singular. El afectado tendrá derecho como mínimo a obtener información significativa sobre la lógica aplicada, así como la intervención humana, a expresar su punto de vista y a impugnar la decisión sin intervención humana, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o le afecten significativamente de modo similar.
7. Derecho a conocer ulteriores tratamientos a los que se someterán sus datos.
8. Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses.
9. Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
10. Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una autoridad de control. Prorrogable a dos meses.
11. Los derechos se pueden ejercer directamente o por medio de tu representante legal o voluntario.
12. Cabe la posibilidad de que el encargado sea quien atienda la solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincula.

Los derechos que proclaman el Capítulo III del Reglamento (UE) 2016/679 y el Título III de la Ley Orgánica 3/2018 son los que se describen a continuación, en consonancia con el documento de la AEPD de diciembre de 2019 sobre "Guía para pacientes y usuarios de la sanidad":

A) La transparencia e información al afectado: recogido por el artículo 12 del Reglamento (UE) y por el artículo 11 de la Ley Orgánica. Este derecho distingue el hecho de que los datos hayan sido obtenidos del afectado o cuando han sido obtenidos por otras vías. El responsable del tratamiento deberá informar al afectado de la identidad del responsable del tratamiento, la finalidad del tratamiento y la posibilidad de ejercer los derechos de acceso, rectificación, supresión, imitación de tratamiento, portabilidad, oposición y la no elaboración de perfiles. En el supuesto de que los datos hubieran sido obtenidos por otras vías, se deberá informar al afectado las fuentes y categoría de los datos[443].

B) El derecho de acceso: así pues, el derecho de acceso a los datos relativos a la salud implica que el titular tendrá derecho a obtener del responsable del tratamiento

[443] AEPD (2019) "Guía para el cumplimiento del deber de informar". Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf (28/02/2021).

confirmación de si se están tratando o no datos personales suyos y en dicho caso, tener derecho al acceso a estos, es decir tener acceso a la historia clínica, a los datos que están en su tarjeta sanitaria y a los datos de las recetas médicas en poder del Farmacéutico y de la Seguridad Social[444]. El artículo 18 de la Ley 41/2002 reconoce el acceso del paciente a su historia clínica.

Este derecho viene recogido en el artículo 15 del Reglamento (UE) y en el artículo 13 de la Ley Orgánica. Cualquier persona tiene derecho a exigir del responsable de un tratamiento de datos la confirmación sobre si se están tratando datos personales de su titularidad. Se entenderá otorgado el derecho cuando el afectado tenga acceso remoto directo y seguro a la totalidad de sus datos, permanentemente. En cualquier caso, el afectado tendrá derecho al acceso a sus datos personales, a obtener una copia de ellos y a conocer:

1. "la identidad y los datos de contacto del responsable y, en su caso, de su representante,
2. los datos de contacto del delegado de protección de datos, en su caso,
3. los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento,
4. los intereses legítimos del responsable o de un tercero,
5. los destinatarios o las categorías de destinatarios de los datos personales,
6. en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional".

Este derecho tiene una importancia especial, pues tal como afirma el TJUE, resulta indispensable para que el interesado pueda ejercer los derechos de rectificación, supresión, bloqueo y la notificación a los terceros de toda rectificación, supresión o bloqueo de datos[445].

En cuanto a los datos relativos a la salud cabe mencionar que el artículo 16.1 de la Ley 41/2002 determina que los profesionales sanitarios del centro o servicio que realice el diagnóstico o tratamiento del paciente o usuario tendrán acceso a la historia clínica, entendiéndose también con acceso a los datos de la tarjeta sanitaria y de las recetas prescritas.

C) El derecho a la rectificación: recogido por el artículo 16 del Reglamento (UE) y por el artículo 14 de la Ley Orgánica. El derecho de rectificación sobre los datos relativos a la salud inexactos deberá ser realizado por el responsable del tratamiento sin dilación en el tiempo[446]. Este derecho está vinculado al principio de la exactitud de los datos y al de calidad de los datos y de su tratamiento. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una

[444] *Vid. Supra p 325,* capítulo 3.2.3.1., del Título III.

[445] STJUE de 7 de mayo de 2009 (Sala tercera) (asunto C-553/07) apartado 49-52.

[446] *Vid. Supra p 331,* capítulo 3.2.3.2., del Título III.

declaración adicional. Todo ello sin dilación indebida. La AEPD facilita a través de su página web el formulario[447]. Cuando la rectificación se deba realizar sobre datos sanitarios, se estará al criterio del profesional sanitario, en base al documento de la AEPD de diciembre de 2019.

D) El derecho a la supresión: llamado también "derecho al olvido"[448] está recogido por el artículo 17 del Reglamento (UE) y por el artículo 15 de la Ley Orgánica. El derecho de supresión mediante la eliminación de sus datos[449], viene modulado por el artículo 21 de la Ley 41/2002, es decir, está limitado al criterio facultativo y siempre que no afecte a datos necesarios para medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, en base al artículo 9.2.h) del Reglamento (UE) 2016/679. Además, en base a este derecho el interesado tendrá derecho a obtener del responsable del tratamiento la supresión o eliminación de los datos personales inexactos, sin dilación indebida, en los supuestos siguientes:

7. "los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo,
8. el interesado retire el consentimiento en que se basa el tratamiento,
9. el interesado se oponga al tratamiento,
10. los datos personales hayan sido tratados ilícitamente,
11. los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento,
12. los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8 del Reglamento (UE) sobre condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información."

E) El derecho a la limitación del tratamiento: recogido en el artículo 18 del Reglamento (UE) y en el artículo 16 de la Ley Orgánica. El derecho a la limitación del tratamiento en cuanto a los datos relativos a la salud y a los de la persona relacionados con la operativa sanitaria[450], viene los modulado por el artículo 21 de la Ley 41/2002, es decir, está limitado al criterio facultativo y siempre que no afecte a datos necesarios para medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social,

[447] AEPD (2019) Sede electrónica de 20 de julio de 2019. "Derecho de rectificación". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-rectificacion (28/02/2021).

[448] AEPD (2019) Sede electrónica de 20 de julio de 2019. "Derecho de supresión ("al olvido")" Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-supresion-al-olvido (28/02/2021).

[449] *Vid. Infra p. 325,* capítulo 3.2.3.1., del Título III.

[450] *Vid. Infra p. 325,* capítulo 3.2.3.1., del Título III.

en base al artículo 9.2.h) del Reglamento (UE) 2016/679. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación al tratamiento de sus datos de los datos en los siguientes supuestos:

5. "el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos,
6. el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso,
7. el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones,
8. el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado."

La AEPD facilita a través de su página web el formulario[451].

F) El derecho a la portabilidad: recogido por el artículo 20 del Reglamento (UE) y por el artículo 17 de la Ley Orgánica. El derecho a la portabilidad en cuanto debe poder recibir sus datos personales en soporte común[452]. Este derecho viene regulado por el artículo 18 de la Ley 41/2002, mediante el derecho a solicitar una copia de la historia clínica, que será entregada en un plazo máximo de un mes, aunque se puede ampliar el plazo, pudiéndose solicitar también la historia clínica de sus familiares fallecidos, salvo disposición en contra opuesta en vida. La aplicación del artículo 20 del Reglamento (UE) hace extensibles este derecho tanto a los datos de la tarjeta sanitaria como a los datos de las recetas.

No obstante, este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable[453]. El interesado tendrá derecho a obtener y recibir del responsable del tratamiento los datos personales, mediante un formato de uso común y lectura mecánica, cuando:

1. El tratamiento este basado en el consentimiento.
2. El tratamiento se realice por medios automatizados.

La AEPD facilita a través de su página web el formulario[454].

[451] AEPD (2019) Sede Electrónica de 20 de julio de 2919. "Derecho a la limitación del tratamiento". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-limitacion-del-tratamiento (28/02/2021).

[452] *Vid. Infra p.331,* capítulo 3.2.3.2., del Título III.

[453] AEPD (2019) Sede Electrónica de 20 de julio de 2919. "Derecho a la portabilidad". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-portabilidad (28/02/2021).

[454] AEPD (2019) Sede Electrónica de 20 de julio de 2919. "Derecho a la portabilidad". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-portabilidad (28/02/2021).

G) El derecho de oposición: recogido por el artículo 21 del Reglamento (UE) y por el artículo 18 de la Ley Orgánica. El derecho de oposición en cuanto el sujeto puede negarse a que sus datos sean tratados o sometidos a determinados tratamientos[455], viene modulado por el artículo 21 de la Ley 41/2002, es decir, está limitado al criterio facultativo y siempre que no afecte a datos necesarios para medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, en base al artículo 9.2.h) del Reglamento (UE) 2016/679.

   El interesado tendrá derecho a oponerse a que sus datos sean tratados, salvo que el responsable del tratamiento acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. La AEPD facilita a través de su página web el formulario[456].

Con carácter general y en relación a los datos protegidos por el artículo 9 del Reglamento (UE), una vez que el ciudadano legitimado solicita ejercer cualquiera de estos derechos el responsable del tratamiento será quien deberá demostrar que han sido respetados.

En relación con los derechos del menor, en cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de quince años[457] los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de la Ley Orgánica 3/2018.

Los datos sometidos a tratamiento podrán haber sido obtenidos del interesado o no obtenidos del interesado, lo cual hará que el afectado reciba además de la información básica, identidad del responsable del tratamiento y de su representante, en su caso, la finalidad del tratamiento y a la posibilidad de ejercer los derechos, se suministrarán las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos, artículo 15 al 22 del Reglamento (UE) 2016/679.

El titular deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679, aunque lo cierto es que en el área sanitaria "la adopción de decisiones individuales automatizadas" no se dan habitualmente.

[455] *Vid. Infra p. 336,* capítulo 3.2.3.3., del Título III.

[456] AEPD (2019) Sede Electrónica de 20 de julio de 2919. "Derecho a oposición". Disponible en https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-oposicion.pdf (28/02/2021).

[457] *Vid. Supra p. 141,* capítulo 5.3.3.2., del Título I.

Además, el Reglamento (UE) 2016/679 reconoce los siguientes derechos aplicables a cualquier tratamiento y por descontado al tratamiento del artículo 9:

a. Derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, artículo 77 del Reglamento (UE) 2016/679.
b. El derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento. Todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales, artículo 79 del Reglamento (UE) 2016/679.
c. Representación de los interesados. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro, artículo 80 del Reglamento (UE) 2016/679.
d. Derecho a indemnización y responsabilidad. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del Reglamento (UE) 2016/679 tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos, Artículo 82 del Reglamento (UE) 2016/679.

Capítulo 3. Tratamiento de los datos relativos a la salud en el tratamiento de categorías especiales en Reglamento 2016/679 y Ley Orgánica 3/2018

3.1. El tratamiento de los datos relativos a la salud dentro del Reglamento 2016/679 y Ley Orgánica 3/2018

El Reglamento (UE) 2016/679 en su artículo 4, definiciones, delimita lo que entiende por tratamiento. Para el Reglamento tratamiento es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales. Para HIDALGO CEREZO, prácticamente toda interacción con un dato de carácter personal se considera tratamiento[458].

La expresión del artículo 4 es clara, dice, cualquier operación o conjunto de ellas. Por otra parte, concluye, el procedimiento automatizado o el procedimiento no automatizado, es decir, automatizado o aquel que se produce sin que intervenga directamente la persona y el no automatizado el que, bien manualmente o mediante un dispositivo, requiere la intervención de la persona.

El propio artículo 4 menciona un listado de operaciones, en las que incluye: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

El capítulo 5 del Título I comenta que, por una parte, no hay que caer en el error de entender que el Reglamento (UE) y la Ley Orgánica regula el tratamiento de dato informático o del de las redes[459], sino que se refiere a cualquier tipo de dato sea cual sea el soporte que tenga (papel, visual, gráfico, etc.). Por otra parte, comenta que el tratamiento de datos excede en mucho el listado del artículo 4 para el Reglamento (UE) 2062/679, obligando en esta Tesis, a diferenciar tres tipos de tratamientos.

En este orden de cosas, en primer lugar, el tratamiento que incluye a los "Elementos básicos del tratamiento de datos", los que aparecen el artículo 4. En segundo lugar, el tratamiento que incluye a los "elementos complementarios del tratamiento de dato", que se componen por todas las operaciones previas al tratamiento de datos o a operaciones colaterales al tratamiento de datos necesarias para que este sea lícito. En tercer lugar, el tratamiento que incluye a los "elementos adiciones en el tratamiento de datos", es decir, todas las acciones u operaciones adicionales que se pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley orgánica 3/2018 y que no constan ni como elementos básicos ni como elementos complementarios.

El tratamiento de los datos relativos a la salud del Reglamento (UE) 2016/679 se encuentra regulado en el artículo 9 sobre "Tratamiento de categorías especiales de

[458] HILDALGO CEREZO, A. (2016) "Protección de datos de carácter …..", op.cit; p 713.

[459] *Vid. Supra p 116,* capítulo 5.2., del Título I.

datos personales" y en la Ley Orgánica 3/2018 en el artículo 9 sobre "Categorías especiales de datos".

En base al Reglamento (UE) 2016/679, el tratamiento de los datos personales solo es licito en base al cumplimiento de unos requisitos regulados en el artículo 6[460], estas bases jurídica son:

1. Por consentimiento.
2. Por exigencia legal, por contrato o por ley.
3. Por interés vitales de cualquier persona física.
4. Por interés público.
5. Por ejercicio de la autoridad pública.
6. Pro interés legítimo del responsable del tratamiento.

El Reglamento (UE) 2016/679 prohíbe en su artículo 9 el tratamiento de datos personales entre los cuales sitúa a datos relativos a la salud. En el mismo artículo 9.2 se establece los supuestos en los que no se aplica dicha prohibición. De tal forma, que la licitud del tratamiento de las categorías especiales de datos se consigue a través de 2 vías: cuando hay consentimiento o cuando no hay consentimiento. Cuando no hay consentimiento tiene que concurrir uno de estos supuestos: exigencia legal, contrato o por ley, intereses vitales de cualquier persona física, interés público o ejercicio de la autoridad pública.

Las excepciones que el Reglamento opone a la exigencia del consentimiento por parte del afectado para la legitimación de terceros para el tratamiento de los datos personales de categoría especial vienen recogidas en el artículo 9.2. Como ya contemplaba la Directiva 95/46/CE estas excepciones hacen referencia al siguiente listado:

- "Limitan el afecto y alcance del consentimiento del afectado cuando el tratamiento esté prohibido por el Derecho de la Unión Europea o por las Leyes de los países miembros. Lo cual indica que se hace referencia a los relativos a los derechos fundamentales recogidos en la Carta de los Derechos Fundamentales de la Unión Europea y en el Tratado de Funcionamiento de la Unión Europea.
- En el marco del cumplimiento de los obligaciones y derechos en el ámbito laboral relativas al responsable del tratamiento o al afectado.
- En situaciones, no estando el afectado esté incapacitado física o jurídicamente para dar su consentimiento, de proteger intereses vitales.
- En el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.

[460] *Vid. Supra p 142,* capítulo 5.4., del Título I.

- Cuando el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.
- Cuando el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial."

Por otra parte, también es cierto que en el apartado 2 del mismo artículo 9, se dice que no se aplicará el punto 1 del artículo 9 en las siguientes circunstancias:

a. "el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b. el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
c. el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d. el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e. el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
f. el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
g. el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h. el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i. el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria

y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional, 4.5.2016 L 119/38 Diario Oficial de la Unión Europea ES

j. el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado."

Lo cual se resume en que, no se aplicará el contenido del artículo 9.1 cuando: el interesado muestre su consentimiento libre; cuando peligre su vida o la de un tercero; cuando intermedia una sentencia judicial; para fines médicos, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social; por razones de interés público o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios.

3.2. Tratamiento de datos relativos a la salud

3.2.1. Tratamiento de los datos relativos a la salud con carácter general

Tal como ya se ha expresado en el capítulo 5.3 del Título I, en el contexto del Reglamento (UE) y de la Ley Orgánica 3/2018, hablar de tratamiento de datos es referirse a los elementos básicos del tratamiento de datos, a los elementos complementarios del tratamiento y los elementos adicionales en el tratamiento de datos personales.

En este orden de cosas, los elementos básicos del tratamiento de datos que como ya se ha visto en el capítulo 5.3.1 del Título I, son: todas las operaciones directas sobre datos que se pueden producir sobre los datos personales y que requieren de protección por parte del Reglamento (UE) 2016/679 y la Ley orgánica 3/2018 y que aparecen en el artículo 4, definiciones, del Reglamento (UE) 2016/679, artículo 4.2 Reglamento (UE) 2016/679. Artículo 4.1.2). Los elementos básicos contemplan las siguientes operaciones: acceso; adaptación y modificación; conservación; comunicación y difusión; cotejo; destrucción; extracción, consulta y utilización; interconexión; organización y estructuración; recogida y registro de datos; y supresión.

En relación con los elementos complementarios del tratamiento vistas en el capítulo 5.3.2. del Título I, estos son: todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4, definiciones, del Reglamento (UE) 2016/679, en el punto relativo a tratamiento, pero que o son acciones u operaciones previas al tratamiento de los datos personales o son colaterales al tratamiento de datos y a su vez, o que son necesarias para que este tratamiento sea lícito. Los elementos básicos contemplan las siguientes acciones: anonimización y seudonimización; bloqueo; circulación y portabilidad; mantenimiento; minimización; exactitud de datos; rectificación; reidentificación; reutilización; tráfico; y transferencia y transmisión internacional.

A estas dos categorías de elementos del tratamiento también se añaden los elementos adicionales en el tratamiento de datos personales y que como consta en el capítulo 5.3.3. del Título I, son: las acciones u operaciones adicionales que se pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley orgánica 3/2018 o en alguno de ellos. Como elementos adicionales en el tratamiento de datos personales, tal como se refleja en el capítulo 5.3.3. del Título I, se hacen constar la: automatización; confidencialidad y consentimiento; y limitación y oposición.

De tal forma, se aplican todos estos elementos básicos, complementarios y adicionales a las categorías especiales de datos del Reglamento (UE) 2016/679 y Ley Orgánica 3/2018, artículo 9, en ambos.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, trataba los datos relativos a la salud, de la siguiente forma. En primer lugar, los catalogaba de "*datos especialmente protegidos*"[461]. En segundo lugar, los facultativos y resto de profesionales de la salud podían tratar los datos de las personas que acudían a ello, aunque deberían regirse por otro tipo de normativa, concretamente por "*lo dispuesto en la legislación estatal o autonómica sobre sanidad*"[462]. Y, en tercer lugar, eximia de la obligación del consentimiento del interesado cuando el dato debiera ser comunicado a un tercero y se encontrara en el supuesto de "Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica"[463].

La nueva legislación además de no legitimar cualquier tratamiento sino solo los del numerus clausus del artículo 6, además prohíbe el tratamiento de determinados datos, en concreto incluye los datos de salud, tal como aparece en el artículo 9, Tratamiento de categorías especiales de datos personales, del Reglamento (UE) 2016/679.

Por otra parte, también es cierto que en el apartado 2 del mismo artículo 9, se dice que no se aplicará el punto 1 del artículo 9 en los supuestos relacionados con la salud en los siguientes supuestos: cuando el interesado muestre su consentimiento; cuando peligre su vida o la de un tercero; cuando intermedia una sentencia judicial; para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social; y por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en

[461] artículo 7 sobre Datos especialmente protegidos de la Ley Orgánica 15/1999.
[462] artículo 8 sobre Datos relativos a la salud de la Ley Orgánica 15/1999.
[463] artículo 11 sobre la Comunicación de datos de la Ley Orgánica 15/1999.

particular el secreto profesional del artículo 9.3 del Reglamento (UE) 2016/679. Debiéndose tener en cuenta además otras limitaciones.

El artículo 9, a su vez, excluye de la prohibición determinadas circunstancias, es decir, siguen siendo datos de categoría especial pero que una circunstancia ajena permite su tratamiento. El propio Reglamento (UE) se autoimpone una serie de exclusiones de la prohibición del artículo 9 en base a:

1. Circunstancias que afectan a la persona física, afectado o tercero: cuando el interesado haya hecho públicos sus datos personales; Cuando haya consentimiento. Sin embargo, no otorga al consentimiento un valor absoluto; y cuando es necesario para fines de relativos a la salud
2. Circunstancias ajenas a la persona afectada: a. atribuidas por funciones de potestad; b. afectadas por el interés general; y c. otras

Concretamente el artículo 9.2.h) hace mención al tratamiento de los datos relativos a la salud en los siguientes términos:

> "el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;"

Hace referencia también a datos relativos a la salud:

> "i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional"

Indirectamente también hace referencia a los datos relativos a la salud al referirse a la investigación científica al decir:

> "j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

De manera también indirecta este apartado del artículo 9 también hace referencia a los datos relativos a la salud, diciendo:

> "g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo

> perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;"

La Ley Orgánica 3/2018 en su artículo 9, sobre categorías especiales de datos, se remite al Reglamento (UE) 2016/679 y en especial en lo referente al tratamiento de los datos relativos a la salud entiende que:

> "Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.
>
> En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte."

Aunque la Ley Orgánica 3/2018 realmente ordena el tratamiento de los datos de salud en su Disposición adicional decimoséptima, sobre tratamientos de datos de salud, creando un verdadero sistema de protección de datos en el ordenamiento jurídico español[464].

Es el artículo 4, Reglamento (UE) 2016/679, el que define tratamiento de datos a efecto del ordenamiento jurídico y a los efectos de la Ley Orgánica 3/2018, pues esta ley orgánica no alberga definición alguna. Tratamiento de datos es, pues, cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. El tratamiento de datos se refiere a cualquier tipo de dato sea cual sea el soporte que tenga sea papel, visual, gráfico o cualquier otro posible. El Tribunal Supremo en sentencia de 2020 entiende que el hecho de que un dato esté en soporte papel o en soporte digital no modifica la calificación de los daños[465].

La aplicación que la Agencia Española de Protección de Datos realiza de esta normativa y que publica en noviembre de 2019 en el documento "Guía para pacientes y usuarios de la sanidad"[466] es la siguiente:

> "No es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para la recogida y utilización de datos personales y de salud si se van a utilizar para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social. (La base de

[464] *Vid. Infra p 268,* capítulo 1.2.4., del Título III.

[465] STS 1614/2020 de 10 de junio de 2020 (Sala de lo Civil), FD 3ª.2 (Desestimación del Recurso).

[466] AEPD (2019) "Guía para pacientes y usuarios de la sanidad". Diciembre 2019. Disposición en https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf (28/02/2021).

> legitimación para este tratamiento de datos está establecida en el artículo 6.1.b) del RGPD para las entidades aseguradoras de salud privadas, y en el artículo 6.1.c) del mismo Reglamento para la sanidad pública)."

Nota Crítica: sorprendentemente para la AEPD, lo dicho hasta ahora, el profesional de la salud en el contexto del artículo 6.1b) del RGPD, sanidad privada, o en el contexto del artículo 6.1.c) del RGPD no estará obligado el solicitar consentimiento a los pacientes para la recogida y utilización de datos personales y de salud.

Tal como dice el preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

> "Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan".

En este orden de cosas, los aspectos claves del ordenamiento jurídico que hacen referencia a la Protección de Datos son tanto los factores, elementos o derechos que protege cómo los elementos efectivos para dicha protección. De esta forma la nueva legislación, Reglamento (UE) 2016/679, eleva la protección del dato personal e incrementa los límites a su tratamiento, entendiendo por tal, su recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

En base a este Reglamento (UE) 2016/679, como datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro y tal como ya se ha comentado en el capítulo 1.2.3.2. del Título III, toda la información de la persona registrada con ocasión de la prestación del servicio sanitario:

> "Todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro."[467]

Este Reglamento 2061/679 entra de lleno en el "consentimiento", reforzando las exigencias del mismo en relación a la normativa derogada, declarando, a su vez, que debe darse mediante un "acto afirmativo claro" que refleje una manifestación de

[467] Directiva 2011/24/UE del Parlamento Europeo y del Consejo.

voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal, artículo 7 del Reglamento (UE) 2016/679. El silencio, las casillas ya marcadas en los formularios o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.

Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento[468]. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo, debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas[469].

Por último, el Reglamento (UE) 2016/679 establece que los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños. El artículo 8 del Reglamento (UE) 2016/679 "Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información" establece la edad de 16 años como edad límite para la licitud de tratamientos de sus datos, en este orden de cosas el artículo reza:

> "1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó".

3.2.2. Disposición adicional decimoséptima de Ley Orgánica 3/2018

La Disposición adicional decimoséptima se basa en el tratamiento de datos relacionados con la salud y en el tratamiento de datos en la investigación en salud. Esta disposición se denomina, tratamiento de los datos de salud.

[468] "Las normas de la carga de la prueba deben cohonestarse con el principio de facilidad probatoria (cuando a una de las partes le resulta fácil probar el hecho controvertido y no lo hace) y con el de la posibilidad probatoria (ya que no es posible exigir pruebas que resulten difíciles o de imposible realización)." STSJ Castilla-León 4320/2019 de 30 de octubre de 2019 (Sala de lo contencioso), FD 4º.

[469] STJUE de 11 de noviembre de 2020 (Sala Segunda) (asunto C-61/19), apartados 39, 40 y 52.

Los aspectos del tratamiento de los datos de salud de la disposición se remiten al Reglamento (UE) 2016/679 concretamente a las letras g), h) i) y j) del artículo 9.2.

La disposición adicional decimoséptima hace referencia no tan solo a los datos estrictamente del campo de la salud sino también a los datos genéticos.

La disposición adicional decimoséptima de la Ley orgánica 3/2018 además de disponer de medidas de seguridad adicionales al tratamiento de datos personales, al recoger toda la normativa sanitaria y de aseguradora configura un complejo sistema de protección[470]. Esta disposición trata, además, integralmente los datos de salud y genéticos comprendidos en los siguientes artículos de las leyes y textos refundidos que se listan a continuación:

a. La Ley 14/1986, de 25 de abril, General de Sanidad en: artículo 18.17; y artículo 55 bis.
b. La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales en: artículo 5.4; y artículo 22.4.
c. La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica en: artículo2.5; artículo 3; artículo 5; artículo 7; artículo 8.3; artículo 9; artículo 10; artículo 14; artículo 15; artículo 16; artículo 17; artículo 18; y artículo 19
d. La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud en: artículo 33.3; artículo 52; artículo 53; artículo 57; artículo 58; y artículo 79.
e. La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias en: artículo 4.9; artículo 4.10; y artículo 5.2.
f. La Ley 14/2007, de 3 de julio, de Investigación biomédica en: artículo 1; artículo 2.c); artículo 3; artículo 4.5; artículo 5; artículo 8; artículo 9.1; artículo 12.2.d); artículo 13; articulo 15.2.d); artículo 15.3; artículo 23; artículo 25.5; artículo 27.3; artículo 34.2.c); artículo 42.2; artículo 44; artículo 45; artículo 47; artículo 48; artículo 49; artículo 50; artículo 51; artículo 52; artículo 53; artículo 58; artículo 59; artículo 66; artículo 67; artículo 69.6; y artículo 70.1.
g. La Ley 33/2011, de 4 de octubre, General de Salud Pública en: artículo 7.2; artículo 9.1; artículo 41.2; y artículo 41.3.
h. La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, en: artículo 99.
i. El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio, en: artículo 17; y artículo 19.4.
j. El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre en: artículo 92; y artículo 104.

[470] BERROCAL LANZAROT, AI. (2019) "Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales". Colección de derecho de las nuevas tecnologías. Madrid. Editorial Reus. p 26.

Los aspectos del tratamiento de los datos en la investigación que establece la Ley orgánica 3/2018 en su Disposición adicional decimoséptima para el uso de datos para la investigación biomédica determina que se podrá dar dicho uso cuando:

1. Es autorizado por el interesado o su representante legal.
2. Los datos están seudonimizados, siempre y cuando exista un compromiso expreso de confidencialidad y de no tan solo de no realizar ninguna actividad de reidentificación, sino que se hayan adaptado las medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. A todo lo cual hay que añadir que se haya producido o exista una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. Deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial y en su defecto, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.
3. La iniciativa parta de las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública, en situaciones de excepcional relevancia y gravedad para la salud pública.

Los supuestos de reutilización en el contexto de este tipo de datos se rigen por las siguientes premisas:

a. La reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, será licita y compatible cuando además del informe previo de previo favorable del comité de ética de la investigación se realice en áreas científicamente vinculadas con el estudio inicial y cuando para este se dio el consentimiento. Aunque los responsables deberán publicar la información[471] en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos u otros formatos, a los afectados.
b. Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

EL Reglamento (UE) 2016/679 dedica el capítulo IX a las Disposiciones relativas a situaciones específicas de tratamiento, en este capítulo se desarrolla el artículo 89 sobre las garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en su punto 2 dice:

[471] Información que deberá facilitarse cuando los datos personales se obtengan del interesado del artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016

> "Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines."

La disposición adicional decimoséptima la letra d) de su punto 2 dice:

> "Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:
>
> 1º. Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.
>
> 2º. El ejercicio de tales derechos se refiera a los resultados de la investigación.
>
> 3º. La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley."

Para aplicar las excepciones que presenta el artículo 89 del Reglamento (UE) 2016/679, se procederá de la siguiente forma:

1º. Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la Autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2º. Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3º. Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4º. Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

3.2.3. El tratamiento de la historia clínica

En el contexto del Reglamento 2016/679 y de la Ley Orgánica 3/2018, hablar de tratamiento de datos es referirnos a sus elementos básicos, complementarios y adicionales. La Ley 41/2002 introduce además otros nuevos elementos del tratamiento de la información clínica de la historia clínica, estos son los criterios de unidad y de integración, con el objeto de facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial, artículo 15 de la Ley 41/2002.

Con relación a los datos especialmente protegidos relativos a la salud de los pacientes, a datos genéticos o datos biométricos debemos entrar a valorar tanto el dato clínico como los distintos soportes o documentos de utilización de este, es decir: la información clínica, información asistencial, la historia clínica y la documentación clínica.

El artículo 3 de la Ley 41/2002 define la historia clínica como *"*el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial".

Con carácter general el dato que configura la historia clínica está protegido por la ley tanto en su titularidad como en la forma de utilizarla o en quién puede hacerlo y cuándo, lo cual significa que su tratamiento debe remitirse a dicha normativa.

La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, artículo 16.1 de la Ley 41/2002, y, en consecuencia, su tratamiento también. En la historia deben figurar unos datos clínicos considerados esenciales, priorizados, para ser sometidos a actividades de evaluación y mejora[472].

El profesional que tiene a su cargo coordinar la información y la asistencia sanitaria del paciente o del usuario es el médico responsable, con el carácter de interlocutor principal del mismo en todo lo referente a su atención e información durante el proceso asistencial, sin perjuicio de las obligaciones de otros profesionales que participan en las actuaciones asistenciales, artículo 3 de la Ley 41/2002.

Este role de responsable de la historia clínica del paciente obliga, también al médico responsable del paciente, a garantizar al paciente el cumplimiento de su derecho en cuanto a su derecho de información de su proceso clínico asistencial. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle, en base al artículo 4.3 de la Ley 41/2002, además de ser responsables de la propia historia clínica[473]. Así pues, podemos decir que este es el primer nivel de responsabilidad.

Cada centro archivará las historias clínicas de sus pacientes[474]. Son los centros sanitarios los que adoptaran las medidas técnicas y organizativas adecuadas para archivar y

[472] LOPEZ-PICAZO FERRER, J.J. et Al (2002) "Datos clínicos esenciales de la historia clínica de atención primaria: una experiencia de evaluación y mejora". Atención primaria, 30 (2), 92-98. p 97.

[473] STS 3006/2010, de 2 de junio de 2010 (Sala de lo Contencioso), FD 1º.

[474] *Vid. Supra p. …* ,capítulo 1.2.5.1., del Título III.

proteger las historias clínicas y evitar su destrucción o su pérdida accidental, mediante las disposiciones necesarias que aprueben las Comunidades Autónomas, artículo 14.4 de la Ley 41/2002. De esta forma, cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten, artículo 16.2 de la Ley 41/2002. Así pues, podemos decir que este es el segundo nivel de responsabilidad.

Además del primer y segundo nivel de responsabilidad hay un tercer nivel, otro tipo de responsable en lo relativo a la historia clínica, este es la Administración pública sanitaria de la Comunidad Autónoma, lo cual ha sido comentado en el capítulo 1.2.5.1. del Título III.

Además, los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda persona tiene derecho a que se respete su voluntad de no ser informada.

La información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias. Incluso la Directiva 24/2011/UE protege este derecho de acceso, obligando al Estado miembro, donde el paciente esté dado de alta como asegurado, a facilitar el acceso a su historia clínica.

Dentro de los elementos básicos del tratamiento, artículo 4 del Reglamento (UE) 2016/679, se incluyen las operaciones que permitan la recogida, organización, estructuración, extracción, consulta, utilización, comunicación. En este orden de cosas, estos elementos básicos también son derechos para el paciente tal como refleja el artículo 19 de la Ley 41/2002, al decir:

> "tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley."

Resumiendo lo dicho hasta aquí. Hasta este punto se constata que el tratamiento de la historia clínica es responsabilidad del facultativo, en su primer nivel, teniendo a su cargo la coordinación de la información del paciente y la obligación de dar cuenta de esta información al propio paciente. Para que esto sea posible cada centro asistencial pondrá a su disposición sistemas de archivos, seguridad, conservación y la recuperación de la información, lo cual sitúa a la Dirección Gerencia del centro sanitario como otro responsable, en su segundo nivel. Así mismo, la Administración pública sanitaria de la Comunidad autónoma aparece como el tercer responsable, en su tercer nivel de responsabilidad. Si pues, hay tres niveles de responsables, el facultativo, como responsable del dato como reflejo de su actividad asistencial, el centro asistencial, como responsable material de la gestión del tratamiento de los datos y la Comunidad Autónoma como responsable de dotar a los centros sanitarios de medidas técnicas y organizativas adecuadas.

En el Capítulo 1.2.5.1 del Título III, se define que la historia clínica es un sistema de datos que comprende el conjunto de documentos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, artículo 3 de la Ley 41/2002, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos. De la historia clínica emanan distintos documentos que si bien nacen de ella tienen distinta naturaleza y tendrán distintos tipos de tratamiento.

El informe de alta es uno de los documentos principales que emanan de la historia clínica, que viene a ser como un resumen cualificado del proceso, con su inicio y su final. El informe de alta médica viene definido en el artículo 3 de la Ley 41/2002, como:

> "el documento emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas."

El informe de alta, una vez emitido forma parte de la historia clínica del paciente.

En este orden de cosas el artículo 20 de la Ley 41/2002 reconoce el derecho de todo paciente, familiar o persona vinculada a él, en su caso, a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial, un informe de alta con los contenidos mínimos que determina el artículo 3. Las características, requisitos y condiciones de los informes de alta se determinarán reglamentariamente por las Administraciones sanitarias autonómicas, artículo 3 de la Ley 41/2002.

El tratamiento del informe de alta, al igual que la historia clínica es responsabilidad del médico que le atendió, quien deberá emitirlo. Así pues, el único responsable del informe de alta será el facultativo asistencialmente responsable del proceso del paciente que le obligó a acudir el centro sanitario.

Finalmente, hay otro tipo de documento que se emite con datos pertenecientes a la historia clínica, estos son los certificados médicos. En este orden de cosas este tipo de comentos con datos personales de categorías especiales aparecen en el artículo 22 de la Ley 41/2002 como un derecho. Así dice: "todo paciente o usuario tiene derecho a que se le faciliten los certificados acreditativos de su estado de salud. Éstos serán gratuitos cuando así lo establezca una disposición legal o reglamentaria."

En base a la clasificación que se realiza del tratamiento de datos del RGPD en el capítulo 5 del Título I, se desarrollaran los siguientes puntos relativos al tratamiento de los datos de la historia clínica.

3.2.3.1. Elementos básicos del tratamiento la historia clínica

En el capítulo 5.3.1 del Título I, se han tratado los elementos básicos del tratamiento de datos y se han definido como las operaciones o acciones que venimos a llamar elementos básicos son: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por

transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

El contenido mínimo de la historia clínica será: la documentación relativa a la hoja clínico-estadística, la autorización de ingreso, el informe de urgencia, la anamnesis y la exploración física, la evolución, las órdenes médicas, la hoja de interconsulta, los informes de exploraciones complementarias, el consentimiento informado, los informe de anestesia, el informe de quirófano o de registro del parto, el informe de anatomía patológica, la evolución y planificación de cuidados de enfermería, la aplicación terapéutica de enfermería, el gráfico de constantes y el informe clínico de alta; del artículo 15 de la Ley 41/2002.

Elementos básicos, en base al Reglamento (EU) 2016/679 y a la Ley 41/2002, aplicados al tratamiento de los datos e información de todo el contenido de la historia clínica es ordenado por orden alfabético, exclusivamente los relativos al Reglamento (UE) 2016/679 se disponen de la siguiente manera:

1. Acceso: si bien el "*acceso*" es una expresión que consta en el Reglamento (EU) 2026/679 en su artículo 4.2 *como "difusión o cualquier otra forma de habilitación de acceso"* se entiende que acceso y difusión son cosas bien distintas. De esta forma se trata el "acceso" en primer lugar, por entender que muchos de los elementos básicos del tratamiento requieren de acceso al dato.

   Se entiende por acceso a la historia clínica el hecho que conduce a que una persona pueda ver y/o leer los datos en ella contenidos y es incuestionable la capacidad del paciente al acceso a su propia documentación clínica con las limitaciones legalmente establecidas[475].

   La persona titular de la historia clínica tiene derecho al acceso a su historia clínica, artículo 18 de la Ley 41/2002.

   Tendrán acceso a la historia clínica las/los profesionales sanitarios del centro o servicio que realice el diagnóstico o tratamiento del paciente, artículo 16.1 de la Ley 41/2002, y es el centro sanitario el que establecerá el método de acceso, artículo 16.2 de la Ley 41/2002.

   El acceso con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia estará a lo dispuesto por la legislación vigente en protección de datos y por lo establezca la Ley 14/1986, General de sanidad, en cualquier caso, asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para anonimizarlos y exceptuando los casos de la el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, los que consten en cualquier autorización judicial y los que sean necesarios para la prevención[476] de

[475] SISO MARTIN, J (18 y 19 abril 2017) "La historia clínica. …..", op.cit; p 15.

[476] Ley 33/2011, de 4 de octubre, General de Salud Pública.

un riesgo o peligro grave para la salud de la población, artículo 16.3 de la Ley 41/2002.

El acceso a la historia clínica informatizada. En este caso el acceso se realiza a través del sistema informático y/o Internet y puede acceder la persona titular de esta historia clínica y el profesional autorizado, En la práctica habitual en el SNS, la historia clínica permite el acceso de todos los profesionales a la misma, a través del icono "registros de accesos". A tal efecto el Servicio de Salud correspondiente debe facilitar la página web de acceso. Se accede con la tarjeta sanitaria Individual (TSI). La identificación de la persona se deberá realizar a través de los medios electrónicos que ofrezca su Comunidad o Ciudad Autónoma, tal como DNI electrónico, Certificado Electrónico emitido por una autoridad de certificación de confianza, o claves concertadas a través de la plataforma Cl@ve[477].

2. Adaptación o modificación: la adaptación o modificación de datos e información se hará por el médico responsable del paciente o de un proceso determinado en cuanto a los datos clínico-médicos o por el personal de enfermería a cargo del paciente, en cuanto a datos de cuidados y procedimientos llevados a cabo por enfermería. Las adaptaciones o modificaciones tendrán que ser suscritas por quien las realice.

3. Comunicación por transmisión: este supuesto solo se da cuando la historia clínica está en soporte informático y el paciente u otro centro asistencial, que esté tratando al paciente, solicita la transmisión de la historia clínica.

   En todo caso, la circulación de la historia clínica en soporte papel corresponde al Servicio de Documentación Clínica del centro sanitario. Cada centro sanitario organizará la comunicación por transmisión, en el caso del Hospital Universitario la Paz (Anexo GG) una vez que el paciente este dado de alta y realizado el correspondiente informe médico, la historia clínica se enviará al Archivo en un plazo menor a 24 horas, si ha sido utilizada en consultas externa, y de 48 horas las procedentes de hospitalización.

4. Conservación: la conservación de los datos e información corresponde al responsable de la gestión del centro asistencial mediante la dotación de recursos para su conservación. En el caso de las historias clínicas en soporte papel, mediante los adecuados archivos de historias clínicas, mientras que, en el caso de historias clínicas informatizadas, mediante la adecuada disposición de sistemas de almacenamiento y copias de seguridad.

   La conservación de la historia clínica es definida como la acción de mantener la historia clínica en condiciones que garanticen su correcto mantenimiento y

[477] MS. Ministerio de Sanidad. "historia clínica Digital del Sistema Nacional de Salud. Preguntas frecuentes. Ciudadanos" www.mscbs.gob.es/ciudadanos/portada/preguntas_frecuentes.htm (31/01/2021).

seguridad, aunque no necesariamente en el soporte original, para la asistencia del paciente[478].

El tiempo mínimo de conservación en España es de 5 años desde la fecha de alta de cada proceso asistencial, artículo 17 de la Ley 41/2002. En la Comunidad Valenciana, artículo 22 de la Ley 1/2003 de 28 de enero[479], en la Comunidad Autónoma de Galicia, artículo 20 de la Ley 3/2001 de 28 de mayo[480] y en el País Vasco, artículos 9 y 10 del Decreto 38/2012 de 13 de marzo[481], el periodo de cinco años también se aplica tras la muerte del paciente, aunque contempla la conservación indefinida en algunos casos. En Cantabria, artículo 72 de la Ley 7/2002, de 10 de diciembre[482] el plazo mínimo de conservación es de quince años, a lo cual se añaden excepciones. En Cataluña, Ley 16/2010, de 3 de junio[483], y en Navarra, Ley Foral 11/2002, de 6 de mayo[484], el plazo mínimo son veinte años desde la muerte del paciente, aunque trascurridos dos años de la última asistencia se podrán destruir aquellos documentos que no sean relevantes para el paciente.

5. Consulta: la consulta solo y exclusivamente se puede realizar por personal sanitario que este atendiendo al paciente durante el proceso de asistencia de este. Para otras consultas deberá existir bien consentimiento, bien estar en algún supuesto de legitimidad previsto en el artículo 9 del Reglamento (UE) 2016/679 o bien que concurran los supuestos del artículo 16 de la Ley 41/2002 en los puntos 3, 4, 5 y 6. La sentencia del Tribunal Supremo de 23 de septiembre de 2015, confirma la prisión a un médico por consultar el historial clínico de cinco compañeros sin consentimiento de estos, condenado por delito de descubrimiento y revelación de secretos[485]. El Tribunal Supremo en sentencia el 1 de marzo de 2021 condena a dos años de prisión a una enfermera del Servicio Aragonés de Salud por acceder al historial clínico de una antigua amiga[486].

   La persona titular de los datos puede consultar los documentos de la historia clínica informatizada. Estos documentos son: historia clínica Resumida; Informe Clínico de Alta; Informe Clínico de Consulta Externa; Informe Clínico de Urgencias; Informe Clínico de Atención primaria; Informe de Cuidados de Enfermería;

[478] CURIEL HERRERO, J., ESTÉVEZ LUCAS, J. (2003) "Manual para la gestión sanitaria y de la historia clínica hospitalaria". Madrid. Ed. Editores Médicos. pp 89-94.

[479] Ley 1/2003, de 28 de enero, de derechos e información al paciente de la Comunidad Valenciana.

[480] Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes.

[481] DECRETO 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.

[482] Ley 7/2002, de 10 de diciembre, de Ordenación Sanitaria de Cantabria.

[483] Ley 16/2010, de 3 de junio, de modificación de la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica.

[484] Ley Foral 11/2002, de 6 de mayo, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica de Navarra.

[485] STS 648/2015 de 23 de septiembre de 2015 (Sala de lo Penal).

[486] STS 743/2021, de 1 de marzo de 2021 (Sala de lo Penal).

Informe de Resultados de Pruebas de Laboratorio; Informe de Resultados de Pruebas de Imagen; e Informe de Resultados de Otras Pruebas Diagnósticas[487].

6. Cotejo: este proceso no se da en las historias clínicas pues no existe el supuesto. Si se diera sería excepcional y se le aplicaría el criterio general relativo al acceso y a la consulta.

7. Difusión o cualquier otra forma de habilitación de acceso: la historia clínica nunca de difunde y su acceso se ha tratado en el anterior punto 1.

8. Destrucción: el proceso de destrucción de la historia clínica está muy vinculado por una parte a su conservación y, por otra parte, a la supresión, lo que el Reglamento (UE) 2016/679 en su artículo 17 viene a llamar derecho al olvido. Sin embargo, la eliminación de los datos de la historia clínica está sometida a limitaciones. La destrucción de los datos se producirá tras el bloqueo de estos, en el caso de que se pudiera bloquear su tratamiento, una vez el bloqueo concluya, artículo 32,2 de la Ley Orgánica 3/2018. Ver también expurgo[488].

9. Estructuración: la historia clínica está estructurada en base a la Ley 41/2002[489], y en función de lo que disponga cada uno de los centros sanitarios. Cumpliendo los mínimos legales que estipula la Ley 41/2002, los centros sanitarios podrán incorporar documentos a la historia clínica, siendo lo habitual que se establezca un procedimiento a tal efecto controlado por la Comisión de Documentación Clínica (Anexo HH).

10. Extracción: la extracción de datos e información de la historia clínica solo se podría realizar su estuviera justificada por el personal que tiene acceso a la misma o por el titular de la misma. Esta extracción, entendida como extraer datos de la historia clínica para otra función está limitada por las reglas del artículo 9 del (UE) Reglamento 2016/679 y la Disposición adicional decimoséptima de la Ley Orgánica 3/2018.

11. Interconexión: la interconexión de datos e información de la historia clínica tan solo tiene sentido en los casos de investigación epidemiológica y se estará a lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica 3/2018. En el supuesto de que se esté refiriendo a la historia clínica informatizada, tendría sentido en el caso de que el sujeto titular o autorizado pueda tener acceso personal y exclusivo desde cualquier punto de la red de Internet a los datos e información de la historia clínica. En este caso esta interconexión está exclusivamente vinculada al titular de dicha información o a persona autorizada o a un caso de urgencia o extrema necesidad.

[487] MS. Ministerio de Sanidad. "historia clínica Digital del Sistema Nacional de Salud. Preguntas frecuentes. Ciudadanos" www.mscbs.gob.es/ciudadanos/portada/preguntas_frecuentes.htm (31/01/2021).
[488] *Vid Infra p 340*, capítulo 3.2.3.4, del Título III.
[489] *Vid Supra p 269*, capítulo 1.2.5.1., del Título III.

12. Limitación: la limitación de datos e información en la historia clínica no podrá ser impuesta por terceros a los responsables de introducirla. El derecho de limitación del tratamiento que reconoce el artículo 18 del Reglamento (UE) 2016/679, debe ser matizado pues puede chocar con artículo 6.1.c y 6.1.d. del Reglamento (UE) 2016/679. De tal forma el artículo 2.5 de la Ley 41/2002 dice:

> "Los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria."

En el supuesto de que el paciente quiera limitar el tratamiento de sus datos en su historia clínica el responsable bien podría oponerse o bien podría negarse, en su caso, a atender al paciente. En el supuesto de que el paciente no posibilite el proceso que le lleve a su diagnóstico y tratamiento se le propondrá su alta voluntaria, si se negara se podrá en conocimiento del juez, artículo 21 de la Ley 41/2002.

La persona titular de los datos puede limitar u ocultar cierta información contenida en la historia clínica informatizada del Sistema Nacional de Salud, aunque en determinadas circunstancias el profesional responsable de su atención sanitaria pude revertir la restricción[490].

13. Organización: la organización de los datos e información de la historia clínica está regulada en su aspecto básico por el artículo 15, contenido de la historia clínica de cada paciente, de la Ley 41/2002. Sin embargo, los centros asistenciales podrán incorporar más elementos y podrán organizar su contenido de la forma que mejor entiendan, siempre y cuando se realice con criterios de unidad e integración, artículo 15.4 de la Ley 41/2002.

14. Recogida: la recogida de datos e información se hace mediante entrevista con el paciente, mediante observación y auscultación, toma o medida de constantes y a través de los datos o información que suministra la tecnología especializada en diagnóstico. Los que recogen los datos son profesionales de la salud o personal auxiliar bajo las órdenes de dichos profesionales, sometidos al deber de secreto profesional, es decir, al secreto profesional sobrevenido[491].

15. Registro: el registro de dato e información en la historia clínica corresponde exclusivamente al profesional que esté atendiendo o, incluso, también al personal auxiliar que esté a su cargo. Debe constar en la historia clínica la identidad del profesional que la introduce.

[490] MS. Ministerio de Sanidad. "historia clínica Digital del Sistema Nacional de Salud. Preguntas frecuentes. Ciudadanos" www.mscbs.gob.es/ciudadanos/portada/preguntas_frecuentes.htm (31/01/2021).
[491] *Vid. Supra p 370*, capítulo 3.4., del Título III.

16. Supresión: la supresión de datos implica su destrucción o eliminación. La supresión de datos y de la información en el ámbito sanitario y concretamente en la historia clínica está muy limitado por los motivos ya comentados el punto "limitación".

    La supresión está muy controlada, solo podrá producirse siempre que no afecte a lo dispuesto en la Ley 41/2002, para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.

    En cuanto a la historia clínica los centros dispondrán de los pertinentes formatos de solicitud de cancelación, como, por ejemplo, refleja la circular para solicitar cancelación de datos del Instituto Psiquiátrico José German del Servicio Madrileño de Salud de la (Anexo II).

17. Utilización: la utilización de la historia clínica está ligada a la licitud de quien accede a ella y de la voluntad de su titular, paciente o usuario sanitario. En este orden de cosas, nos remitimos a la operación de acceso y a cualquier otra operación que se encamine a manejar los datos en interés de alguien. Los interesados solo pueden ser los titulares de la información o también como consta en el Reglamento (UE) 2016/679 cualquier tercero autorizado por el artículo 9, es decir, por la autoridad pública en bien de un tercero por estar comprometida su salud, individual o colectivamente, o por orden judicial, en bases a cuestiones de interés general.

3.2.3.2. Elementos complementarios del tratamiento la historia clínica

En el capítulo 5. 2 del Título I, se han tratado los elementos complementarios del tratamiento de datos. Si bien, por una parte, esta Tesis entiende a los elementos básicos del tratamiento de datos como todas las operaciones y acciones incluidas en el artículo 4 del Reglamento (UE) 2016/679, por otra parte, describe y define los elementos complementarios del tratamiento, como todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4.2), definiciones, del Reglamento (UE) 2016/679. Estos elementos complementarios son: acciones u operaciones previas al tratamiento de los datos personales; o acciones u operaciones colaterales al tratamiento de datos; o que son acciones u operaciones necesarias para que este tratamiento sea lícito.

Estos elementos complementarios que aparecen en el Reglamento (UE) 2016/679 y/o la Ley Orgánica 3/2018 comprenden: la anonimización y seudonimización; el bloqueo; la circulación y portabilidad; el mantenimiento; la minimización; la exactitud de datos; rectificación; la reidentificación; reutilización; tráfico; y la transferencia y transmisión internacional.

Elementos complementarios, en base al Reglamento (EU) 2016/679 y a la Ley 3/2018, aplicados a la historia clínica constan, ordenado por orden alfabético, en el listado siguiente. A la derecha del texto consta la norma en la que el elemento está contemplado:

1. Anonimización: la anonimización de la historia clínica equivale a despojarla de cualquier identificación que pueda definir a una persona. Dato anónimo y anonimizado es lo mismo, "son aquellos datos respecto de los que no es conocida la identidad de la persona a la que se refieren ni es posible su identificación"[492]. (Ley Orgánica 3/2018)

   Esta práctica no es utilizada salvo estudios de investigación en los cuales el paciente o usuario no haya dado su consentimiento.

   La anonimización de la historia clínica debería ser autorizada por el facultativo responsable del paciente en el mismo sentido que en el caso de la limitación del tratamiento de los datos o bien solicitarla una copia para luego anonimizarla. La anonimización convierte a la historia clínica en un documento inútil desde el punto de vista del titular de los datos.

2. Bloqueo: el bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas, artículo 32.2 de la Ley Orgánica 3/2018. (Ley Orgánica 3/2018)

   El bloqueo de la historia clínica se lleva a cabo bien custodiando el documento bajo llave y responsabilidad personal de la misma mediante un código de encriptación, en el caso de que se trata de una historia clínica digitalizada. Es habitual que las historias clínicas de personas trabajadoras de los propios centros sanitarios estén bloqueadas. Está estrechamente vinculado a la cancelación[493].

3. Exactitud: la exactitud en los datos de una historia clínica es una condición fundamental en su registro. En este sentido, cuando la historia clínica esta automatizada la historia clínica lleva incorporados códigos incompatibles, como por ejemplo sería que el dato de varón o hembra pudiera ser cambiado en un proceso de un parto, o que en un servicio de geriatría pudiera introducirse en el campo de la edad, un valor de 14 o 15 años. (Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018)

[492] GÓMEZ PIQUERAS, C. (2009) "Disociación/anonimización de los datos de salud". Revista Derecho y Salud, 18 (1), 43-56. p 47.

[493] GALLEGO RIESTRA, S. (2016) "Los derechos de acceso, rectificación, cancelación y oposición del paciente sobre su historia clínica". Revista Derecho y salud, 26 (1), 133-140. p 139.

4. Circulación: las historias clínicas tienen sus propios circuitos dentro de los centros asistenciales. El control de la circulación, movimiento y uso de dicha documentación será responsabilidad del Servicio de Documentación Clínica o Servicio con denominación similar, artículo 17.4 de la Ley 41/2002.

   Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   El Archivo de historias clínicas tiene como objetivo fundamental guardar y custodiar la documentación clínica que generen los pacientes. Un ejemplo es el Hospital Universitario La Paz, en el cual una vez dado el paciente de alta y realizado el correspondiente informe médico, la historia clínica se enviará al Archivo historias clínicas de en un plazo menor de 24 horas, si ha sido utilizada en consultas externas, y de 48 horas las procedentes de hospitalización (Adenda 1).

5. Mantenimiento: mantenimiento y conservación son términos muy cercanos. En este orden de cosas, desde el punto de vista de las actividades generales del mantenimiento, este puede ser: mantenimiento de conservación y mantenimiento de actualización. El manteamiento de conservación hace referencia tiene a reparar los deterioros provocados por el uso. El manteamiento de actualización tiene a compensar la obsolescencia y nuevas exigencias. También se distingue entre manteamiento predictivo, preventivo y correctivo[494].

   Ley Orgánica 3/2018

   Aplicar esta teoría a la historia clínica conlleva las técnicas que se utilizan para su mantenimiento físico tanto en los archivos donde se almacenan las historias clínicas como durante el transporte de estas y su almacenamiento.

   Un defecto en el mantenimiento podría afectar negativamente a los derechos de la persona, entre otros, al derecho de la persona de poder acceder a sus datos personales y a todos los derechos vinculados con su limitación, oposición y destrucción.

6. Minimización: el artículo 5.1.c) del Reglamento (UE) 2016/679 entiende como minimización de datos: adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Está vinculado a la conservación de los datos[495], elemento básico número 4 del capítulo 3.2.3.1. del Título III.

   Reglamento (UE) 2016/679

   En la historia clínica este elemento complementario del tratamiento, la minimización, no se puede tener en cuenta sin el

[494] GARCÍA GARRIDO S. (2003) "Organización y gestión integral del mantenimiento". Madrid. Ed. Diaz de Santos. p 17.

[495] BELTRÁN AGUIRRE, JL (2018) "Reglamento general …..", op.cit; p 74-76, p 87.

criterio del facultativo responsable de la historia clínica, artículo 15.2 de la Ley 41/2002, el cual es el que determina el alcance de este concepto, aunque también se tendrá que escuchar el criterio de la Administración sanitaria, artículo 14.3 de la Ley 41/2002, en cuanto a la minimización de datos en la historia clínica. Aunque se sobreentiende que en la historia clínica no debe constar datos que no sean necesarios, artículo 15 de la Ley 41/2002.

El artículo 15 de la Ley 41/2002 dice:

> "La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. De a la forma que el criterio que deberá regir en la historia clínica es el de criterio de necesidad sobre el de minimización."

7. Portabilidad: se trata de que la persona interesada reciba los datos personales que haya facilitado a un responsable del tratamiento para transmitirlos a otro responsable del tratamiento sin que el primero de ellos se lo impida. Este proceso del tratamiento se realizará en un formato estructurado, de uso común y lectura mecánica. Todo ello cuando haya mediado consentimiento por parte de la persona interesada y los datos estén en soporte informático. Además de ser un elemento complementario del tratamiento de la historia clínica, es un derecho reconocido por el artículo 20 del Reglamento (UE) 2016/679, derecho de portabilidad de los datos.

   Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   La portabilidad de la historia clínica sea cual sea su soporte, en la Ley 41/2002 viene reflejada como el derecho a solicitar una copia de la historia clínica, artículo 18 de la Ley 41/2002. Esta copia será entregada en un plazo máximo de un mes, aunque se puede ampliar el plazo, pudiéndose solicitar también la historia clínica de sus familiares fallecidos, salvo disposición en contra opuesta en vida[496].

8. Rectificación: la rectificación además de ser un elemento complementario del tratamiento de los datos de la historia clínica en base al Reglamento (UE) 2016/679, artículo 16, es también un derecho de la persona cuando sus datos no son exactos o están incompletos y una obligación del responsable del tratamiento[497]. En cuanto a la historia clínica los centros dispondrán de los pertinentes formatos de solicitud de rectificación, tal como refleja la circular

   Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

[496] AEPD (2019) "Guía para pacientes y usuarios de la sanidad". Diciembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf (28/02/2021).

[497] GALLEGO RIESTRA, S. (2016) "Los derechos de acceso, rectificación, cancelación y oposición del paciente sobre su historia clínica". Revista Derecho y salud, 26 (1), 133-140. p 139.

para solicitar rectificación del Instituto Psiquiátrico José German del Servicio Madrileño de Salud Adenda 2.

9. Reidentificación: la reidentificación no está permitida en el caso de los datos del artículo 9 del Reglamento (UE) 2016/679 y tal como dice la Ley 3/2018, no está permitida en los datos de salud, Disposición adicional decimoséptima, sobre tratamientos de datos de salud. Ley Orgánica 3/2018

   En este aspecto el apartado 2, de la Disposición adicional decimoséptima, introduce medidas preventivas frente a la reidentificación de datos seudonimizados. Además, exige el compromiso escrito de los profesionales implicados de que no se van a reidentificar datos seudonimizados.

10. Reutilización: volver a utilizar datos identificables que ya se han utilizado para fines de investigación biomédica. Este tratamiento es licito cuando se dispone del consentimiento de la persona afectada, Disposición adicional 17ª de la Ley Orgánica 3/2018, o cuando coincidan con la finalidad concreta del consentimiento dado para su utilización científica o de investigación biomédica, Disposición transitoria 6ª de la Ley Orgánica 3/2018. Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

11. Seudonimización: la seudonimización es una actividad que separa el dato de la persona titular a través de un código, de tal forma, que el dato no se pueda imputar a tu titular[498]. Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

    En el caso de la historia clínica se aplicará esta técnica cuando se lleven a cabo investigaciones biomédicas sin el consentimiento expreso del titular del dato y se cumplan los requisitos del apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica 3/2018. 2016/679 y la Ley Orgánica 3/2018

    El Reglamento (UE) 2016/679 entiende que la seudonimización es un criterio de licitud del tratamiento de datos personales cuando no se cuente con el consentimiento de la persona. En este caso, el Reglamento (UE) equipara la seudonimización con el cifrado de datos.

12. Tráfico: el tráfico de datos de la historia clínica se limita a los siguientes supuestos: Ley Orgánica 3/2018

    a. Cuando una persona quiera copia de su historia clínica del centro donde la tienen archivada.

[498] MIRALLES LÓPEZ, R. (2017) "Desvinculando datos personales: seudonimización, desidentificación y anonimización". Revista de la Sociedad Española de Informática y Salud, 122, pp 7-9.

b. Cuando un centro sanitario que atiende a un paciente solicita la historia clínica al centro donde la tienen archivada.
c. Cuando una persona desde su ordenador personal accede a su historia clínica informatizada.

En estos casos hay tráfico de los datos de la historia clínica. En todos ellos se deberán cumplir los criterios de licitud del acceso y se deberán exigir que estén activos sistemas de seguridad digital.

Si la información se solicitara desde un tercer país de la Unión Europea el sistema a aplicar sería el que rige para las transferencias internacionales.

13. Transferencia: este supuesto se remite a lo mismo que lo dicho en el supuesto del tráfico.

    El reglamento dedica un gran espacio y varios artículos a la transferencia de datos entre países miembros de la Unión Europea y entre estos y terceros países.

Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

14. Transmisión internacional: este supuesto se remite a lo mismo que lo dicho en el supuesto del tráfico a lo que hay que añadir que las Transferencias de datos personales a terceros países u organizaciones internacionales está regulado por el Capítulo V, del artículo 44 al 50, del Reglamento (UE) 2016/679.

    Se estará a lo determinado para las transferencias basadas en una decisión de adecuación y a sus excepciones[499].

Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

3.2.3.3. Elementos adicionales en el tratamiento la historia clínica

En el capítulo 5. 3 del Título I, se ha descrito, dentro del tratamiento de datos personales, la categoría de los elementos adicionales en el tratamiento de datos.

Si bien esta Tesis entiende a los elementos básicos del tratamiento de datos como a todas las operaciones y acciones incluidas en el artículo 4 del Reglamento (UE) 2016/679, y por otra parte, describe y define los elementos complementarios del tratamiento, como todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4.2), definiciones, del Reglamento (UE) 2016/679, también entiende los elementos adicionales en el tratamiento de datos como las acciones u operaciones adicionales, que no son ni básicas ni complementarias, que se pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley orgánica 3/2018 o en alguna de estas dos normas.

[499] *Vid Supra p. … ,*capítulo 1.2.2.1, del Título II.

Estos elementos adicionales que aparecen en el Reglamento (UE) 2016/679 y/o la Ley Orgánica 3/2018 comprenden: automatización, confidencialidad, consentimiento y oposición.

Los elementos adicionales, en base al Reglamento (EU) 2016/679 y a la Ley 3/2018, aplicados a la historia clínica constan, ordenado por orden alfabético, en el listado siguiente, el cual describe a la derecha del texto la norma en la que el elemento está contemplado:

1. automatización: el Reglamento (UE) 2016/679 al referirse a tratamiento automatizado se refiere al que tiene soporte informático y lo diferencia del tratamiento manual. El Reglamento (UE) relaciona la automatización con la elaboración de perfiles. Aunque, el Reglamento (UE) 2016/679 dice en su Considerando 15: Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   > "A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas".

   La automatización de la historia clínica se refiere bien a la historia clínica generada en soporte digital utilizando cualquier herramienta informática o bien a la historia clínica en soporte papel que se ha digitalizado posteriormente. El tratamiento automatizado es el que no es manual[500].

2. Confidencialidad: es relativo al principio de intimidad y reserva de la información y datos que contiene la historia clínica, en su totalidad o en parte. Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   El tratamiento de los datos de la historia clínica deberá ser siempre realizado respetando la máxima confidencialidad, reserva o secreto. Si bien la confidencialidad no es un tratamiento, es una forma de realizarlo, es decir, tratamiento confidencial.

   Esta forma de tratar los datos se establece como un deber en el artículo 15 de la Ley 3/2018 y del artículo 5 del Reglamento (UE) 2016/679. Tal como dice el artículo 5.2 de la Ley Orgánica 3/2018, el deber de confidencialidad será complementario al deber de secreto profesional.

3. Consentimiento: el consentimiento en lo relativo a la historia clínica es una cuestión clave. Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y Ley 41/2002

   Para acceder a los datos de una historia clínica siempre se debe contar con el consentimiento del paciente salvo que la persona que accede este legitimada por la norma o salvo que la situación en la se

[500] *Vid. Supra p 37*, capítulo 1.4., del Título I.

encuentre el interesado o terceras personas autorice la actuación, artículo 9.2 y artículo 6 del Reglamento (UE) 2016/679.

En este orden de cosas, incluso ningún médico puede acceder a la historia clínica de una persona sin una razón profesional, bien porque sea el médico que atiende a la persona o bien porque la afección del titular de la historia clínica puede afectar la salud de terceras personas, artículo 16 Ley 41/2002, aplicable también post-morten. El consentimiento está vinculado al derecho a la intimidad, artículo 7 Ley 41/2002.

El consentimiento para acceder a los datos de una persona es una condición general que impone el Reglamento (UE) 2016/679, sean de la naturaleza que sean, determinado las bases jurídicas el artículo 6 del Reglamento (UE) 2016/679, es decir, en que situaciones se puede acceder.

Estas condiciones de licitud del artículo 6 se superponen a las condiciones del artículo 9 del Reglamento (UE) 2016/679 al concretar las bases jurídicas para el tratamiento de categorías especiales de datos personales, entre los que incluye cualquier dato relativo a la salud de una persona.

El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública no requiere el consentimiento del interesado, artículo 16 Ley 41/2002 y artículo 9.2. del Reglamento (UE) 2016/679.

4. Oposición: el elemento de oposición al tratamiento de los datos de la historia clínica está reconocido como derecho por el artículo 21 del Reglamento (UE) 2016/679 y por los concordantes de la Ley 3/2018.

Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

Cuando se ha estudiado el derecho a la supresión[501] se ha mencionado que este derecho está limitado por el criterio del médico responsable en base a que este puede entender que la información que se quiere eliminar puede ser necesaria para salud o seguridad del paciente o para la salud de terceras. Sin embargo, la oposición al tratamiento no significa la destrucción de estos. Incluso el artículo 21 del Reglamento (UE) 2016/679 entiende que el interesado se puede oponer aun cuando se alegue el artículo 6.1.e) y el artículo 6.1.f) salvo que se acrediten motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

[501] *Vid. Supra p 103,* capítulo 2.3., del Título I.

En el caso concreto de la historia clínica cabrían supuestos de que el interesado fuera trabajador del propio centro, que profesionales vinculados con su proceso tuvieran relación de amistad o parentesco con el paciente, o casos similares, en cuyo caso el titular de los datos podría oponerse a determinados tratamientos de su historia clínica o que determinadas personas pudieran realizarlos.

Algunos autores entienden que la oposición en la historia clínica vendría dada cuando el paciente muestra "oposición a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención" [502].

3.2.3.4. Otros elementos del tratamiento la historia clínica distintos de los encontrados en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018

La Ley 41/2002 introduce además otros de los elementos del tratamiento de la información clínica de la historia clínica, estos son el archivo, la custodia, la integración y la unidad documentales.

Se introducen además otros elementos del tratamiento de la historia clínica tales como la custodia, el archivo y el expurgo de la historia clínica, que aparece en el Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica, del País Vasco.

Estos nuevos elementos del tratamiento son:

1. Archivo: cada centro sanitario archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizada su seguridad, su correcta conservación y la recuperación de la información, artículo 14 de la Ley 41/2002.

   La Ley 41/2002 y el Decreto 38/2012, del País Vasco

   El archivo, en sus depósitos, deberán tener condiciones de seguridad, restricción de acceso, control de accesos y monitorización de estos.

   El archivo de historia clínica se puede externalizar, en cuyo caso se deberá tomar las debidas precauciones, en este orden de cosas, en el País Vasco se determina que los contratos de externalización dispondrán de la garantía de cumplimiento de la normativa vigente.

   Esta externalización del archivo debería soportarse en un contrato de encargado, artículo 14 de la Ley 41/2002, no pudiendo subcontratar el encargado con otro encargado sin autorización del responsable, artículo 28.2 del Reglamento (UE) 2016/679.

[502] GALLEGO RIESTRA, S. (2016) "Los derechos de acceso, rectificación, cancelación y oposición del paciente sobre su historia clínica". Revista Derecho y salud, 26 (1), 133-140. p 138.

2. Custodia: dejar constancia del acceso y uso de la historia clínica. En el caso de País Vasco, el Decreto 38/2012 especifica que se anotará, nombre, apellidos y documento nacional de identidad (DNI) de la persona que ha accedido a la historia clínica, naturaleza del acceso, que incluirá contenido y justificación, y fecha del acceso. Asimismo, se anotarán las restricciones practicadas al acceso por razón de la protección de la identidad de la persona paciente, los derechos de terceras personas a la confidencialidad de los datos que constan en la historia clínica en interés terapéutico del o de la paciente o los derechos de los y las profesionales participantes en su elaboración.

   La Ley 41/2002 y el Decreto 38/2012, del País Vasco

   La custodia de las historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario[503] y los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen, artículos 17.4 y 17.5 de la Ley 41/2002.

   En este orden de cosas, la custodia como un elemento del tratamiento de la historia clínica es reconocida como un derecho por la Ley 41/2002, introduciendo el concepto de custodia activa, la cual será la que permita la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley, del artículo 19 de la Ley 41/2002.

3. Expurgo: es el proceso de evaluación crítica y selección de los soportes y tipos documentales de la historia clínica que reúnen las mejores condiciones de testimonio e información para poder determinar la continuidad de su conservación y la retirada o destrucción de aquellos que no sean esenciales para resumir y reconstruir cada episodio asistencial.

   Relativos al Decreto 38/2012, del País Vasco

   El expurgo se podrá realizar una vez pasados los plazos de conservación de la historia clínica.

4. Integración: la integración de datos e información dentro de la misma estructura de información del interesado está vinculada a los criterios de acceso.

   Relativos a la Ley 41/2002

   Si se pretende integrar los datos e información de una historia clínica con los de otra, solo tendría sentido dentro del marco de la investigación biomédica, la cual está regulada por la Disposición adicional decimoséptima de la Ley Orgánica 3/2018.

[503] SANCHEZ-CARO J., ABELLAN F. (2003) "Derechos y deberes …..", op.cit; pp 13,71.

La Ley 41/2002, entiende que la historia clínica está dirigida a obtener la máxima integración de la documentación clínica del paciente, artículo 14 de la Ley 41/2002, y que se llevará con criterio de integración, artículo 15 de la Ley 41/2002.

5. Unidad: la unidad en la información del paciente es un criterio que justifica y explica la historia clínica.

Relativos a la Ley 41/2002

La Ley 41/2002, contempla este criterio en el artículo 15.

3.2.4. El tratamiento de la receta

El capítulo 1.2.5.2 del Título III, sobre la receta y la recta electrónica del Sistema Nacional de Salud describe la receta ordinaria y la receta especial. La recta ordinaria, tanto en su vertiente médica, receta, como en su vertiente de enfermería, orden de dispensación, y la recta electrónica del Sistema Nacional de Salud. La receta especial, la que se utiliza para la dispensación de estupefacientes.

Tal como dice el capítulo 1.2.5.2 del Título III la receta médica es el documento de carácter sanitario, normalizado y obligatorio mediante el cual los médicos, odontólogos o podólogos, legalmente facultados para ello, y en el ámbito de sus competencias respectivas, prescriben a los pacientes los medicamentos o productos sanitarios sujetos a prescripción médica, para su dispensación por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas o, conforme a lo previsto en la legislación vigente, en otros establecimientos sanitarios, unidades asistenciales o servicios farmacéuticos de estructuras de atención primaria, debidamente autorizados para la dispensación de medicamentos, del Real Decreto 1718/2010.

La receta llevará datos inexcusables para su validez así pues datos relativos al paciente, datos relativos la medicamento, datos del prescriptor y otros datos, artículo 3 del Real Decreto 1718/2010.

En este orden de cosas, parece que no cabe duda de que los datos de la receta están sometidos al tratamiento del artículo 9 del Reglamento (UE) 2016/679[504].

La historia clínica tal como se ha visto en el capítulo 1.2.5.1. del Título III es, tal vez, el documento relativo a la salud más relevante, pero no el único. La historia clínica de un paciente contiene todos los episodios de atención de la persona con el sistema sanitaria y cada episodio puede ser atendido por un profesional distinto. Sin embargo, la receta vincula al paciente con dos profesionales, es un solo documento individual, el facultativo que lo emitió y en el caso del orden de prescripción, el enfermero/a que lo ordenó, y el farmacéutico que los dispensa..

[504] AEPD (2020) "Datos de Salud en dispositivos móviles y seguridad jurídica". La Solución DocToDoctro. Disponible en https://www.aepd.es/sites/default/files/2020-02/premio-2019- emprendimiento-Molinapps. pdf (31/01/2021).

Los datos de la receta nacen cuando se emiten y están íntimamente relacionados con la historia clínica, incluso pueden nacer de ella, del tratamiento, pero la receta no forma parte de la historia clínica. La naturaleza de la receta es temporal, nace cuando se emiten los datos en el documento, receta, y su fin se agota al ser dispensado, pues el farmacéutico utiliza dichos datos para el acto de dispensación. En el caso de las recetas de la Seguridad Social, esta entidad pública también someterá la receta a tratamiento de datos a la hora de financiar el medicamento. Tal como ya se explicó en el capítulo 1.2.5.2. del Título III.

La receta es pues un documento con datos personales relativos a la salud de una persona que tiene tan solo un responsable, pero que su naturaleza y esencia se perfecciona por el uso del documento de un profesional distinto del primero que la emitido, estamos refiriéndonos al farmacéutico. Por tanto, en el supuesto de la receta se debe tener en cuenta que es un documento que tiene dos responsables del tratamiento de estos datos, por una parte, el responsable de la emisión de los mismos y por otra parte el responsable del tratamiento final de los mismos.

El Gobierno determinará con carácter básico los requisitos mínimos que han de cumplir las recetas médicas extendidas y/o editadas en soporte informático con el fin de asegurar la accesibilidad de todos los ciudadanos, en condiciones de igualdad efectiva en el conjunto del territorio español, a la prestación farmacéutica del Sistema Nacional de Salud, artículo 79 de la Real Decreto Legislativo 1/2015[505].

No será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, de conformidad con lo dispuesto en el artículo 9.2 letra h) del Reglamento (UE) 2016/679. Las citadas actuaciones deberán tener por finalidad facilitar la asistencia médica y farmacéutica al paciente y permitir el control de la prestación farmacéutica del Sistema Nacional de Salud, artículo 79.8 del Real Decreto Legislativo 1/2015.

> "Artículo 7. Datos especialmente protegidos.
>
> 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
>
> 6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
>
> Artículo 8. Datos relativos a la salud.

[505] Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

> Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.
>
> Artículo 11. Comunicación de datos.
>
> 1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
>
> 2. El consentimiento exigido en el apartado anterior no será preciso:
>
> a) Cuando la cesión está autorizada en una ley."

La Información de las recetas será suministrada por las Consejerías responsables de las Comunidades Autónomas al Ministerio de Sanidad que efectuará la agregación y depuración correspondiente antes de hacerla pública, lo cual recibe la denominación de "Gestión de información sobre prestación farmacéutica del Sistema Nacional de Salud", por parte del artículo 106 del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

El fin de esta autorización legal es posibilitar la valoración de la prescripción y de la política farmacéutica general, para lo cual Administración pública competente facilitará la información agregada o desagregada relativa al consumo de medicamentos tanto por receta como a nivel de centros hospitalarios y cualesquiera otros ámbitos incluidos dentro de la prestación farmacéutica del Sistema Nacional de Salud, artículo 106 del Real Decreto Legislativo 1/2015. Lo cual se realizará salvando siempre la confidencialidad de la asistencia sanitaria y de los datos comerciales de empresas individualizadas.

Nótese que el artículo 106 del Texto Refundido, dice "información agregada", lo que indica que al no ser una información que identifique a la persona no es de aplicación el Reglamento (UE) 201//679. Sin embargo, añade también que se puede transmitir información desagregada, lo cual, en este supuesto, hace comparecer de nuevo al Reglamento (UE) 2016/679. Aunque también indica este artículo 106 que se realizará salvando la confidencialidad.

En cuanto a la protección de datos en las recetas médicas y órdenes de dispensación hospitalaria, una vez entrado en vigor del Reglamento (UE) 2016/679 no es necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico en base al artículo 9.2 letras b) y h) del Reglamento (UE) 2016/679 en base al artículo 79.8 del Real Decreto Legislativo 1/2015. Aunque, quedará garantizada la confidencialidad de la asistencia médica y farmacéutica, la intimidad personal y familiar de los ciudadanos y la protección de sus datos de carácter personal en función del artículo 9.3 del Reglamento (UE9 2016/679 y del artículo 19 del Real Decreto 1718/2010. Sin embargo, el paciente podrá solicitar en el momento de la prescripción de las recetas electrónicas, una especial protección y confidencialidad en la

dispensación del tratamiento, debiéndose diferenciar la dispensación, pudiéndose realizar a través de receta en soporte papel o a través de los procedimientos que se determinen por las Administración sanitaria, artículo 8 del Real Decreto 1718/2010.

La Disposición adicional decimoséptima, sobre tratamientos de datos de salud, de la Ley Orgánica 3/2018 menciona 10 Leyes relativas a datos de salud, sin embargo, no hace ninguna mención a la Ley 16/1997, de 25 de abril, de Regulación de Servicios de las oficinas de farmacia ni al Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación. La poca alusión a la protección de datos en relación a las recetas conlleva a que sea de aplicación exclusivamente el Reglamento (UE) 2016/679.

En conclusión, en este caso, debe entenderse que es de aplicación el artículo 9.2 y 9.3 del Reglamento (UE) 2016/679 a todos los efectos de las recetas tengan el soporte que tengan.

3.2.4.1. Elementos básicos del tratamiento de la receta

Tal como ya se ha comentado en el capítulo 5.3.1 del Título I, se han tratado los elementos básicos del tratamiento de datos y se han definido como las operaciones o acciones que venimos a llamar elementos básicos y que son: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

El contenido mínimo de la receta será como consta en el capítulo 1.2.5.2.1. del Título III, el contenido del artículo 3 del Real Decreto 1718/2010 que es el que se describe: datos del paciente; datos del medicamento; datos del prescriptor; y otros datos. Estos son de forma detallada:

A) Datos del paciente: el nombre, dos apellidos, y año de nacimiento; en las recetas médicas de asistencia sanitaria pública, el código de identificación personal del paciente, recogido en su tarjeta sanitaria individual, asignado por su Servicio de Salud o por las Administraciones competentes de los regímenes especiales de asistencia sanitaria[506]. En las recetas médicas de asistencia sanitaria privada, el número de DNI o NIE del paciente; en el caso de que el paciente no disponga de esa documentación se consignará en el caso de menores de edad el DNI o NIE de alguno de sus padres o, en su caso, del tutor, y para ciudadanos extranjeros el número de pasaporte.
B) Datos del medicamento: denominación del principio/s activo/s o denominación del medicamento; dosificación y forma farmacéutica y, cuando proceda, la mención de los destinatarios: lactantes, niños, adultos; Vía o forma de administración, en caso necesario; formato: número de unidades por envase o contenido del mismo en peso o volumen; número de envases o número de unidades concretas del medicamento a dispensar; posología: número de unidades

[506] En el caso de ciudadanos extranjeros que no dispongan de la mencionada tarjeta, se consignará el código asignado en su tarjeta sanitaria europea o su certificado provisional sustitutorio (CPS) o el número de pasaporte para extranjeros de países no comunitarios y en todo caso se deberá consignar, asimismo, el régimen de pertenencia del paciente

de administración por toma, frecuencia de las tomas, por día o semana o mes, y duración total del tratamiento.

C) Datos del prescriptor: el nombre y dos apellidos; población y dirección donde ejerza; número de colegiado o, en el caso de recetas médicas del Sistema Nacional de Salud, el código de identificación asignado por las Administraciones competentes y, en su caso, la especialidad oficialmente acreditada que ejerza[507]; la firma será estampada personalmente una vez cumplimentados los datos de consignación obligatoria y la prescripción objeto de la receta y en las recetas electrónicas se requerirá la firma electrónica, que deberá producirse conforme con los criterios establecidos por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

D) Otros datos: la fecha de prescripción, día, mes, año: fecha del día en el que se cumplimenta la receta; la fecha prevista de dispensación, día, mes, año: fecha a partir de la cual corresponde dispensar la receta, en el caso de dispensaciones sucesivas de tratamientos crónicos o medicamentos de dispensación renovable; Número de orden: número que indica el orden de dispensación de la receta, en el caso de dispensaciones sucesivas de tratamientos crónicos o medicamentos de dispensación renovable.

Los elementos básicos del tratamiento, en base al Reglamento (EU) 2016/679 y a la Ley 41/2002, aplicados al tratamiento de los datos e información de todo el contenido de la receta es, ordenado por orden alfabético:

1. Acceso: si bien el "acceso" es una expresión que consta en el Reglamento (EU) 2026/679 en su artículo 4.2 como "difusión o cualquier otra forma de habilitación de acceso" se entiende que acceso y difusión son cosas bien distintas. De esta forma se trata el "acceso" en primer lugar, por entender que muchos de los elementos básicos del tratamiento requieren de acceso al dato. Se entiende por acceso a la receta el hecho que conduce a que una persona pueda ver y/o leer los datos en ella contenidos.

   Tendrán acceso a la receta del paciente en base al artículo 9 del Reglamento (UE) 2016/679 cualquier profesional sujeto a la obligación de secreto profesional. La licitud para el acceso a los datos de la receta vendrá dada bien por el artículo 9 del Reglamento (UE) 2016/679 o bien por los prescriptores a los que se refiera el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios. De esta forma se hace referencia al enfermero y fisioterapeutas prescriptores, podólogo, el farmacéutico o personal auxiliar y el médico que le haya recetado y el profesional sanitario sanitarios que por exigencias de su puesto de trabajo y función asistencial tenga la necesidad de conocer el contenido de la receta.

[507] En las recetas médicas de la Red Sanitaria Militar de las Fuerzas Armadas, en lugar del número de colegiado podrá consignarse el número de Tarjeta Militar de Identidad del facultativo. Asimismo, se hará constar, en su caso, la especialidad oficialmente acreditada que ejerza.

2. Adaptación o modificación: la adaptación o modificación de datos en la receta tan solo podrá realizarla el prescriptor. Sin embargo, con carácter excepcional, cuando concurran las cusas establecidas por la Ley, el farmacéutico podrá sustituir el dato del fármaco por otro, el de menor precio, artículo 89.2 del Real Decreto Legislativo 1/2015.

3. Comunicación por transmisión: la transmisión de la receta se producirá en el caso de la receta electrónica y siguiendo las normas protección de la confidencialidad de los datos, artículo 11 del Real Decreto 1718/2010. Se seguirá lo establecido con carácter general por el RGPD.

4. Conservación: la conservación de las rectas corresponde al farmacéutico, artículo 1 de la Ley 16/1997, durante un plazo de tres meses, artículo 18.3 del Real Decreto 1718/2010 o por el paciente. En el caso de las recetas de psicótropos el plazo de conservación es de cinco años, artículo 17 del Real Decreto 1675/2012.

5. Consulta: la receta solo podrá ser consultada por el prescriptor o por el farmacéutico o personal delegado en las oficinas de farmacia. Se seguirá lo establecido con carácter general por el RGPD y por el secreto profesional[508].

6. Cotejo: este proceso no se da en las recetas pues no existe el supuesto. Si se diera sería excepcional y se le aplicaría el criterio general relativo al acceso y se seguirá lo establecido con carácter general por el RGPD.

7. Difusión o cualquier otra forma de habilitación de acceso: la receta nunca de difunde y su acceso se ha tratado ya en el punto 1.

8. Destrucción: pasado el plazo de conservación el farmacéutico procederá a la destrucción de la receta utilizando métodos que garanticen la imposibilidad de la reconstrucción del documento. Las recetas médicas de medicamentos estupefacientes o psicotrópicos y aquellas otras que deban ser sometidas a procedimientos de ulterior gestión o control, serán tramitadas por el farmacéutico de acuerdo con las normas e instrucciones específicas aplicables en cada caso, en el caso de los psicótropos deberán pasar cinco años.

9. Estructuración: viene estructurada por la Administración pública con competencias en sanidad y farmacia.

10. Extracción: la extracción de datos e información de la receta solo afecta al formato electrónico y le corresponde al farmacéutico y al personal de la farmacia delegado a las funciones de dispensación.

11. Interconexión: la interconexión de datos e información de la receta tan solo tiene sentido el formato de la receta electrónica.

[508] *Vid. Supra p 145*, capítulo 5.5 del Título I y *Vid. Infra p 375*, capítulo 3.4.4.2., del Título III.

12. Limitación: la limitación de datos e información en la receta no podrá ser impuesta por terceros a los responsables de tratarla.

    El derecho de limitación del tratamiento que reconoce el artículo 18 del Reglamento (UE) 2016/679, cuando se pretende aplicar a la receta, debe ser matizado pues puede chocar con artículo 6.1.c y 6.1.d. del Reglamento (UE) 2016/679.

    En el supuesto de que el paciente quiera limitar el tratamiento de sus datos en su recta, el responsable del tratamiento bien podría oponerse o bien podría negarse, en su caso, se le aplicaría el derecho del paciente a la negación al tratamiento contemplada en el artículo 2.4 de la Ley 41/2002, excepto que en los casos que se negará, se aplicaría el artículo 21 de la Ley 41/2002 y se podrá en conocimiento del juez, artículo 2.4 de la Ley 41/2002.

    La persona titular de los datos puede limitar u ocultar cierta información contenida en la recta informatizada del Sistema Nacional de Salud, aunque en determinadas circunstancias el profesional responsable de su atención sanitaria pude revisar la restricción, artículo 8 del Real Decreto 1718/2010.

13. Organización: la organización de los datos e información de la recta está regulada por el anexo de criterios básicos de las recetas médicas y órdenes de dispensación, del Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.

14. Recogida: la recogida de datos e información la hace el prescriptor.

15. Registro: el registro de dato e información en la receta corresponde exclusivamente al prescriptor.

16. Supresión: la supresión de datos implica su destrucción o eliminación por petición del titular de los datos.

    La supresión de datos y de la información en el ámbito sanitario y concretamente en la receta están muy limitado por los motivos ya comentados el punto “limitación”.

    La supresión está muy limitada, y vinculada al derecho de negarse al tratamiento del artículo 2.4 de la Ley 41/2002 y con el alta forzosa del artículo 21 de la Ley 41/2002.

17. Utilización: la utilización de la receta está ligada a la legitimidad de quien accede a ella en la oficina de dispensación o farmacia.

3.2.4.2. Elementos complementarios del tratamiento de la receta

En el capítulo 5.3.2 del Título I, se han tratado los elementos complementarios del tratamiento de datos. Si bien esta Tesis entiende a los elementos básicos del tratamiento de datos como a todas las operaciones y acciones incluidas en el artículo 4

del Reglamento (UE) 2016/679, por otra parte, también describe y define los elementos complementarios del tratamiento, como todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4.2, definiciones, del Reglamento (UE) 2016/679. Estos elementos complementarios son: acciones u operaciones previas al tratamiento de los datos personales; o acciones u operaciones colaterales al tratamiento de datos; o que son acciones u operaciones necesarias para que este tratamiento sea lícito.

Estos elementos complementarios que aparecen en el Reglamento (UE) 2016/679 y/o la Ley Orgánica 3/2018 comprenden: la circulación y portabilidad; el mantenimiento; la minimización; la exactitud de datos; rectificación; tráfico; y la transferencia y transmisión internacional. En relación con la historia clínica no se incluyen los siguientes elementos complementarios: la anonimización, el bloqueo, la reidentificación, la reutilización y la seudonimización.

Elementos complementarios, en base al Reglamento (EU) 2016/679 y a la Ley 3/2018, aplicados a la receta constan (ordenado por orden alfabético) en el listado siguiente, a la derecha del texto consta la norma en la que el elemento está contemplado:

1. Exactitud: la exactitud en los datos de una receta es una condición fundamental en su registro.

   Le corresponde al prescriptor atender a este tratamiento, sin embargo, se entiende que este tratamiento también podrá ser llevado a cabo por el farmacéutico en su caso, en base al artículo 1.2 y 1.8 de la Ley 16/1997, de 25 de abril, de Regulación de Servicios de las oficinas de farmacia.

   Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

2. Circulación: las recetas tienen sus propios circuitos dentro de los centros asistenciales dirigidos a la farmacia del centro y cuando es una receta a dispensar por la oficina de farmacia en formato papel la circulación le corresponde al paciente o persona en la que delegue.

   Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

3. Mantenimiento: mantenimiento y conservación son términos muy cercanos.

   El mantenimiento antes del acto de la dispensación por parte de la Oficina de Farmacia le corresponde al titular de los datos o al paciente, una vez dispensado el medicamento le corresponde al farmacéutico de la Oficina de Farmacia, artículo 1.1 de la Ley 16/1997.

   Ley Orgánica 3/2018

4. Minimización: este tratamiento de datos no tiene sentido aplicado a la receta pues la estructura de datos está impuesta por la normativa, sin embargo, en el apartado de observaciones deberá aplicarse el criterio de minimización. En el caso de las recetas del

   Reglamento (UE) 2016/679

sector privado, el prescriptor deberá limitar los datos y observaciones a lo estrictamente necesario.

5. Portabilidad: en este caso se atiende a lo dicho para la circulación. La posibilidad de llevar o portar la receta no tiene ningún tipo de condición cuando la ejerce el titular de la misma, cualquier otra portabilidad no es posible y requiere la autorización del titular, excepto la que realice el farmacéutico en cumplimiento de sus funciones. Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

6. Rectificación: la rectificación de la receta tan solo puede producirse por el prescriptor o con carácter excepcional, cuando concurran las causas establecidas por la ley, el farmacéutico podrá sustituir el fármaco por otro, el de menor precio, artículo 89.2 del Real Decreto Legislativo 1/2015. Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

7. Tráfico: el tráfico de datos de la receta se remite a la circulación y a la portabilidad. Por tráfico se hace referencia a una forma de mover, circular o portar la receta que no tiene más limitación que la voluntad del titular de esta, excepto en el caso de que este tráfico sea realizado por el farmacéutico en el cumplimiento de sus obligaciones. Ley Orgánica 3/2018

8. Transferencia: este supuesto se remite a lo mismo que lo dicho en el supuesto del tráfico, circulación o portabilidad de las recetas. La transferencia de recetas no tiene ninguna peculiaridad que no se haya ya reseñado en los otros términos similares. También, se puede entender que al hablar de transferencia el término se refiere a una movilidad producida por una tercera persona ajena al titular, en cuyo caso rige la doctrina del RGPD. Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

9. Transmisión internacional: este supuesto se remite a lo mismo que lo dicho en el supuesto del tráfico a lo que hay que añadir que las transferencias de datos personales a terceros países u organizaciones internacionales está regulado por el Capítulo V (artículo 44 a 50) del Reglamento (UE) 2016/679. Se estará a lo determinado para las transferencias basadas en una decisión de adecuación y a sus excepciones[509]. Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   En cuanto al contenido de los datos que contengan las recetas a efectos de la Sanidad Transfronteriza dentro de la UE se estará a lo que dispone el Real Decreto 81/2014, de 7 de febrero, por el que se

[509] *Vid Supra p 185,* capítulo 1.2.2.1., del Título II.

establecen normas para garantizar la asistencia sanitaria transfronteriza, y por el que se modifica el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.

3.2.4.3. Elementos adicionales en el tratamiento de la receta

En el capítulo 5.3.3 del Título I, se han tratado los elementos adicionales en el tratamiento de datos. Si bien esta Tesis entiende a los elementos básicos del tratamiento de datos como a todas las operaciones y acciones incluidas en el artículo 4 del Reglamento (UE) 2016/679, por otra parte, describe y define los elementos complementarios del tratamiento, como todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4.2), definiciones, del Reglamento (UE) 2016/679, entiende los elementos adicionales en el tratamiento de datos como las acciones u operaciones adicionales, que no son ni básicas ni complementarias, que se pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley orgánica 3/2018 o en alguno de ellos

Estos elementos adicionales que aparecen en el Reglamento (UE) 2016/679 y/o la Ley Orgánica 3/2018 comprenden: automatización, confidencialidad, consentimiento y oposición.

Elementos adicionales, en base al Reglamento (EU) 2016/679 y a la Ley 3/2018, aplicados a la receta son, ordenado por orden alfabético, los que constan en el listado siguiente, a la derecha consta la norma en la que el elemento está contemplado

1. automatización: el Reglamento (UE) 2016/679 al referirse a tratamiento automatizado se refiere al que tiene soporte informático y lo diferencia del tratamiento manual. Lo relaciona con la elaboración de perfiles. Aun así, el Reglamento (UE) 2016/679 dice en su Considerando 15: "A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas". — Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   La automatización de la receta se refiere bien a la receta generada en soporte digital utilizando la herramienta informática oficial o bien a la receta en soporte papel que se ha digitalizado posteriormente. El tratamiento automatizado es aquel que no es manual.

   La automatización de la recta es aplicable a la receta electrónica y viene regulada mediante el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación y por sus posteriores modificaciones[510].

[510] Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza, y por el que se modifica el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.

2. Confidencialidad: si bien la confidencialidad no es un tratamiento, si es una forma de realizarlo, es decir, tratamiento confidencial o aquel realizado con las suficientes medidas que garantizan su no divulgación[511] o su acceso por terceras personas.

Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

Esta forma de tratar los datos se establece como un deber en el artículo 15 de la Ley 3/2018 y del artículo 5 del Reglamento (UE) 2016/679. Tal como dice el artículo 15.2 de la Ley 3/2018, el deber de confidencialidad será complementario al deber de secreto profesional.

El tratamiento confidencial es relativo al principio de intimidad y reserva de la información y datos que contiene la receta, en su totalidad o en parte. De tal forma que el personal sanitario tiene el deber de garantizar la confidencialidad y la intimidad de los pacientes en la tramitación de las recetas y órdenes médicas, artículo 111.2.b). 19ª. Real Decreto Legislativo 1/2015.

El tratamiento de los datos de la receta, electrónica o en papel, deberá ser siempre realizado respetando la máxima confidencialidad, artículo 19 del Real Decreto 1718/2010), reserva o secreto.

En cuanto a la receta electrónica 11 artículo del Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, determina que el sistema de receta médica electrónica garantizará la seguridad en el acceso y transmisión de la información, así como la protección de la confidencialidad de los datos establece un mecanismo adicional de confidencialidad.

El artículo 8 del Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, establece un mecanismo adicional de confidencialidad.

Una vez utilizada la receta esta será custodiada durante 3 meses por el farmacéutico responsable de la oficina de farmacia garantizando su seguridad, correcta conservación y confidencialidad, artículo 18 del Real Decreto 1718/2010.

3. Consentimiento: el consentimiento para acceder a los datos de una persona es una condición general que impone el Reglamento (UE) 2016/679, sean de la naturaleza que sean, estableciendo el artículo 6 del Reglamento (UE) 2016/679 las situaciones lícitas. Estas

Reglamento (UE) 2016/679, la Ley Orgánica

[511] El Tribunal Supremo entiende que cuando una información es confidencial "no podrán ser divulgadas a ninguna persona", así lo trata en la STS 1565/2020 de 19 de noviembre d 2020 (Sala de lo Contencioso-Administrativo), DF 2º (párrafo 8º).

3/2018 y Ley 41/2002

condiciones de licitud del artículo 6 se extreman en los supuestos del artículo 9 del Reglamento (UE) 2016/679 al especificar el tratamiento de categorías especiales de datos personales, entre los que incluye cualquier dato relativo a la salud de una persona.

El acceso a la historia clínica y el acceso a la receta no son situaciones similares, pues el fin de cada uno de estos documentos y los datos que contienen son distintos.

Real Decreto Legislativo 1/2015 entiende en su artículo 79.8 que no será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, lo que cual se relaciona con la causa de exclusión de la condición de consentimiento del titular de la información de los supuestos del artículo 9.2 letra h) del Reglamento (UE) 2016/679.

Por otra parte, el artículo 103, protección de datos personales, del Título VIII, de la financiación pública de los medicamentos y productos sanitarios, del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, establece que no requerirá el consentimiento del interesado para el tratamiento de datos de la receta por el Instituto Nacional de la Seguridad Social o, en su caso, el Instituto Social de la Marina.

La Disposición adicional decimoséptima Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se refiere a la Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios.

A través del artículo 9 del Reglamento (UE) 2016/679, en su apartado 2.h) se deduce que el consentimiento para el tratamiento de los datos de la receta no debería ser exigido en todos los casos.

En el supuesto de las recetas públicas emitidas por el Sistema Nacional de Salud, el consentimiento se podría obviar en consideración del apartado 2.h) del artículo 9.

En el supuesto las recetas en medicina privada el consentimiento vendría condicionado por la relación del paciente o persona con el prescriptor. En el caso de que la persona tuviera una relación contractual con el proveedor de servicios tan solo haría falta que la persona mostrara su consentimiento en el momento de la contratación en base al apartado 1.c) del artículo 6, en caso contrario, se entiende que cada receta debería ser acompañada por el correspondiente consentimiento.

En cuanto al tratamiento de los datos de la receta por parte de la Oficina de Farmacia, se entiende que, en las rectas públicas del Sistema Nacional de Salud, podría aplicarse el apartado 2.h) de artículo 9, sin embargo, cuando la receta es emitida por un médico con actividad privada, la oficina de farmacia debería solicitar el consentimiento del tratamiento a la persona. Si la persona fuera cliente asidua a la misma Oficina de Farmacia, bastaría con suscribir una sola vez el consentimiento para el tratamiento de los datos de las recetas privadas.

Cuando la receta es electrónica, el consentimiento del interesado se entiende dado mediante la lectura de la tarjeta por el lector de tarjetas a disposición de la oficina de farmacia[512].

4. Oposición: el derecho oposición al tratamiento de los datos está reconocido por el artículo 21 del Reglamento (UE) 2016/679 y por los concordantes de la Ley 3/2018/679. Cuando se ha visto el derecho a la supresión, se ha mencionado que este derecho está limitado por el criterio del médico responsable en base a que este puede entender que la información que se quiere eliminar puede ser necesaria para salud o seguridad del paciente o para la salud de terceras. Sin embargo, la oposición al tratamiento no significa la destrucción de los mismos. Incluso el artículo 21 del Reglamento (UE) 2016/679 entiende que el interesado se puede oponer aun cuando se alegue el artículo 6.1.e) y el artículo 6.1.f) salvo que se acrediten motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

   Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   En el caso concreto de la receta se entiende que la oposición actuaría igual que supresión o la limitación.

3.2.4.4. Otros elementos del tratamiento de la receta distintos de los encontrados en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018

Otras normas con rango de Ley y otras con rango de Decreto introducen además otros de los elementos del tratamiento de la información clínica de la receta, estos son la custodia.

1. Custodia: la custodia de la receta corresponde al farmacéutico de la Oficina de Farmacia, artículo 1.2 de la Ley 16/1997.

   Ley 16/1997, de 25 de abril, de Regulación

[512] GIL MEMBRADO, C (2011) " La e-receta: confidencialidad y proyecto de regulación". Revista derecho y salud, 21 (1), 31-60. p 39.

de Servicios de las Oficinas de Farmacia

En cuanto a la custodia de las recetas electrónicas del Sistema Nacional de Salud, esta le corresponde a las Administraciones sanitarias públicas, por lo que garantizarán la custodia de las bases de datos de prescripción y dispensación y establecerán los criterios de autorización y control de acceso a dichas bases de datos, artículo 7.4. del Real Decreto 1718/2010.

3.2.5. El tratamiento de la tarjeta sanitaria

La tarjeta sanitaria es el documento administrativo de reconocimiento del derecho a la asistencia sanitaria de la Seguridad Social[513], y que mediante la acreditación de determinados datos de su titular posibilita el acceso de este a las prestaciones de atención sanitaria que proporciona el Sistema Nacional de Salud, artículo 57 de la Ley 16/2003. Dispone para ello de los datos básicos comunes, el código de identificación personal del Sistema Nacional de Salud y la base de datos de población protegida de dicho sistema, artículo 3 del Real Decreto 183/2004.

La tarjeta sanitaria se ha convertido en un instrumento indispensable para la asistencia sanitaria en el Sistema Nacional de Salud, ya no tan solo para la filiación de la persona sino para el uso de la receta electrónica, siendo "Una de las herramientas fundamentales para la operatividad de la e-receta"[514].

La utilización de la tarjeta sanitaria permite la visualización de los datos que lleva incorporados en su superficie física y la posibilidad de acceso a los datos de la banda magnética de la tarjeta sanitaria la hace susceptible de incluirla en el tema de los datos sanitarios[515], dado que estos datos permiten acceder a información protegida de las personas física y sobre todo permite acceder a información relativa a datos de salud de la persona física.

Tal como ya se ha visto en el capítulo 1.2.5.3 del Título III la tarjeta sanitaria contiene "datos básicos comunes"[516]. El conjunto de los datos de la tarjeta sanitaria configura la Base de Datos de Población Protegida del Sistema Nacional de Salud[517], regulada por el artículo 6 del Real Decreto 183/2004, de 30 de enero.

Al ser la tarjeta sanitaria un documento que porta datos personales le será de aplicación el Reglamento (UE) 2016/679 y la Ley orgánica 3/2018 y todas las normas de protección que le sean de aplicación. También le debería ser de aplicación el tratamiento de categorías especiales de datos dado que la información que posee la tarjea sanitaria es específica para el sistema sanitario público y a través de ella se puede acceder

[513] MISSSM (2020) "Asistencia Sanitaria". Ministerio de Inclusión social, Seguridad Social y Migraciones. Disponible en http://www.seg-social.es/wps/portal/wss/internet/InformacionUtil/44539/45195 . (31/01/2021).

[514] GIL MEMBRADO, C (2011) " La e-receta: confidencialidad y proyecto de regulación". Revista derecho y salud, 21 (1), 31-60. p 39.

[515] *Vid. Supra p 284*, capítulo 1.2.5.3., del Título III.

[516] *Vid. Supra p 285,* capítulo 1.2.5.3.1., del Título III.

[517] *Vid. Supra p 292*, capítulo 1.2.5.3.1.4., del Título III.

automáticamente a datos netamente clínicos, concretamente a través del código de identificación personal[518].

Los datos que contiene la tarjeta sanitaria pueden dar acceso a bases de datos que contienen datos de categorías especiales relativos al artículo 9 del Reglamento (UE) 2016/679 y de la Ley orgánica 3/2018.

En el contexto del Reglamento 2016/679 y de la Ley Orgánica 3/2018, hablar de tratamiento de datos es referirnos a los elementos básicos del tratamiento, a los elementos complementarios del tratamiento y a los elementos adicionales. Como elementos básicos del tratamiento nos remitimos al artículo 4 del Reglamento (UE) 2016/679, que dice que tratamiento de datos es:

> "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."

La Administración pública dispondrá de bases de datos de los usuarios del Sistema Nacional de Salud con tarjeta sanitaria, con información básica y situaciones de aseguramiento, cuyo fin será el de proceder a la generación del código de identificación personal del Sistema Nacional de Salud. Esta base de datos actuará como un sistema de intercambio de información entre las Administraciones sanitarias, con el fin de facilitar la gestión de la población protegida, su movilidad y el acceso a los servicios sanitarios. Incorporará información del sistema de Seguridad Social y del mutualismo administrativo. Estas bases de datos permiten el tratamiento de datos de las situaciones de las personas respecto a altas, bajas, cobertura de prestaciones y movilidad de pacientes en la Unión Europea, de acuerdo con los reglamentos comunitarios vigentes en esta materia.[519]

En el capítulo 1.2.5.4 del Título III, sobre el conjunto mínimo básico de datos del Sistema Nacional de Salud, se analiza el Conjunto Mínimo Básico de Datos al Alta Hospitalaria, que supone un extracto impersonal de información administrativa y clínica, que debe ser recogida a partir del informe de alta. El artículo 5 "Contenido del registro" de Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención sanitaria Especializada, determina que contendrá el Código de Identificación Personal y el número de historia clínica, además de otros datos de carácter personal y de salud.

A través del Código de Identificación Personal o CIP, que está inscrito en la parte frontal delantera de la tarjeta sanitaria y está también grabado en la banda magnética de la parte dorsal trasera de la Tarjeta sanitaria, se puede acceder su puede interrelacionar la persona, con la Base de Datos de la tarjeta sanitaria[520] y a su vez con el Conjunto Mínimo Básico de Datos.

[518] *Vid. Supra p 288,* capítulo 1.2.5.3.1.2., del Título III.

[519] Artículo 5 del Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

[520] *Vid. Supra p 292,* capítulo 1.2.5.3.1.4., del Título III.

El contenido mínimo de la tarjeta sanitaria será como consta en el capítulo 2.5.3.1 del Título III, artículo 3 del Real Decreto 1718/2010, los datos básicos a incluir en el anverso de la tarjeta sanitaria son:

a) Identidad institucional de la comunidad autónoma o entidad que la emite
b) Los rótulos de "Sistema Nacional de Salud de España" y "tarjeta sanitaria"
c) Código de identificación personal asignado por la administración sanitaria emisora de la tarjeta (CIP-AUT)
d) Nombre y apellidos del titular de la tarjeta
e) Código de identificación personal único del Sistema Nacional de Salud (CIP-SNS)
f) Código de identificación de la administración sanitaria emisora de la tarjeta

Las Administraciones Públicas sanitarias emisoras, podrán incorporar además a la tarjeta sanitaria el número del Documento Nacional de Identidad de su titular o, en el caso de extranjeros, el número de identidad de extranjeros, el número de la Seguridad Social, la fecha de caducidad de la tarjeta para determinados colectivos o el número de teléfono de atención de urgencias sanitarias, todos ellos en formato normalizado. Igualmente se podrá incluir una fotografía del titular de la tarjeta sanitaria, en los supuestos en los que así lo autorice la ley y pudiendo poner en el ángulo inferior derecho de la tarjeta sanitaria se grabarán, en braille, los caracteres de las iniciales de tarjeta sanitaria Individual (TSI), artículo 5.3 y 5.4 del Real Decreto 702/2013.

Existe Interoperabilidad plena de las tarjetas sanitarias, en base al Ministerio de Sanidad. Cada ciudadano tiene asignado un Código de Identificación Personal único para todo el SNS. Las CCAA disponen de un sistema de intercambio de datos que permite mantener actualizada la información sobre población protegida en cada comunidad y en el conjunto del SNS.

En el capítulo 5 del Título I, analiza los elementos que componen el tratamiento de datos describiendo los elementos básicos (recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción); los elementos complementarios (acciones u operaciones previas al tratamiento de los datos personales; o acciones u operaciones colaterales al tratamiento de datos; o que son acciones u operaciones necesarias para que este tratamiento sea lícito); los elementos adicionales (automatización, confidencialidad y consentimiento, oposición); y otros elementos no encontrados directamente en el Reglamento (UE) 2016/679 ni en la Ley Orgánica 3/2018.

A continuación de describen estos elementos del tratamiento de la tarjeta sanitaria.

3.2.5.1. Elementos básicos del tratamiento de la tarjeta sanitaria

Tal como ya se ha comentado en el capítulo 2.2 del Título III y en el capítulo 5. 1 del Título I, se han tratado los elementos básicos del tratamiento de datos y se han definido

como las operaciones o acciones que venimos a llamar elementos básicos, que albergan: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Los elementos básicos del tratamiento, en base al Reglamento (EU) 2016/679 y a la Ley 41/2002, aplicados al tratamiento de los datos e información de todo el contenido de la tarjeta sanitaria, ordenado por orden alfabético:

1. Acceso: si bien el "acceso" es una expresión que consta en el Reglamento (EU) 2026/679 en su artículo 4.2 como "difusión o cualquier otra forma de habilitación de acceso" se entiende que acceso y difusión son cosas bien distintas. De esta forma se trata el "acceso" en primer lugar, por entender que muchos de los elementos básicos del tratamiento requieren de acceso al dato. Se entiende por acceso a la tarjeta el hecho que conduce a que una persona pueda ver y/o leer los datos en ella contenidos.

   Tendrán acceso a la tarjeta sanitaria del SNS del paciente, en base al artículo 9 del Reglamento (UE) 2016/679, cualquier profesional sujeto a la obligación de secreto profesional. Este profesional tendrá base legal para el acceso a los datos de la tarjeta sanitaria, artículo 9 del Reglamento (UE) 2016/679.

   A los datos de la tarjeta sanitaria Individual y a la base de datos de población protegida accede la Administración sanitaria en el ejercicio de sus funciones. Es este caso se aplica el apartado 2.h) del artículo 9 del Reglamento (UE) 2016/679.

   Además, tendrá acceso a la tarjeta sanitaria Individual el personal de la oficina de farmacia, artículo 8 y artículo 9 del Real Decreto 1718/2010.

2. Adaptación o modificación: la adaptación o modificación de datos en la tarjeta sanitaria tan solo podrá realizarla la Administración sanitaria autonómica encargada de la emisión de la tarjeta sanitaria, Real Decreto 183/2004.

3. Comunicación por transmisión: la transmisión de los datos de la tarjeta sanitaria en base a lo dispuesto por el Ministerio de Sanidad[521] se produce en todo el territorio nacional a través del Ministerio de Sanidad y sus sistemas de información. La Base de Datos de Población Protegida actúa como un sistema de intercambio de información entre las Administraciones sanitarias, artículo 5.2 del Real Decreto 183/2004. Las oficinas de farmacia utilizarán la tarjeta sanitaria tanto para identificar al paciente como para acceder a la receta electrónica, artículo 8 y artículo 9 del Real Decreto 1718/2010.

[521] MS. Ministerio de Sanidad (2010). "Interoperabilidad plena de las tarjetas sanitarias" Disponible en https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/tic01.htm (31/01/2021).

4. Conservación: la conservación de las tarjetas sanitarias corresponde a la persona titular.

   En cuanto a las Bases de Datos de Población Protegida del Sistema Nacional de Salud, su conservación corresponde la Administración sanitaria emisora de la tarjeta sanitaria Individual, artículo 5.3 del Real Decreto 183/2004.

   Por otra parte, el Ministerio de Sanidad y Consumo, como responsable de la base de datos, aplicará las medidas de seguridad y accesos de conformidad con lo dispuesto en la normativa vigente en protección de datos de personales y por el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, artículo 6.3 del Real Decreto 183/2004.

   Las defunciones de las personas dan de baja a la persona de Base de Datos de Población Protegida como persona protegida.

5. Consulta: la tarjeta sanitaria Individual podrá ser consultada bien por los ciudadanos a través de las webs que ponga a disposición Administración sanitaria emisora de la tarjea sanitaria, o bien cualquier centro de asistencia sanitaria del Sistema Nacional de Salud para constatar la cobertura de la asistencia por la Administración pública y Administración de referencia. Podrá consultar la tarjeta sanitaria las oficinas de farmacia, artículo 5.2. del Real Decreto 1718/2010.

6. Cotejo: este proceso no se da en las tarjetas sanitarias pues no existe el supuesto.

7. Difusión o cualquier otra forma de habilitación de acceso: la tarjeta sanitaria nunca de difunde y su acceso se ha tratado en el anterior punto 1.

8. Destrucción: las tarjetas sanitarias en desuso, en poder de la Administración sanitaria o de cualquier centro sanitario público, serán destruidas al cabo de un mes de su captación. Cada Administración sanitara dispondrá de una Unidad de tramitación de las tarjetas sanitarias o similar, que se encargaran de la destrucción de estas. Las unidades de tramitación no destruyen directamente las tarjetas, sino que son las Gerencias de los centros sanitarios las que formalizarán un contrato con empresa certificada para realizar dicha tarea, y según la Normativa Europea DIN 32757-1.

9. Estructuración: la tarjeta sanitaria viene estructurada por el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

10. Extracción: la extracción de datos e información de la tarjeta sanitaria corresponde a los centros sanitarios del Sistema Nacional de Salud y, en su caso, al farmacéutico y al personal de la farmacia delegado a las funciones de dispensación.

11. **I**nterconexión: la transmisión de los datos de la tarjeta sanitaria en base al Ministerio de Sanidad[522] se produce en todo el territorio nacional a través del Ministerio de Sanidad y sus sistemas de información. La Base de Datos de Población Protegida actúa como un sistema de intercambio de información entre las Administraciones sanitaria, artículo 5.2 del Real Decreto 183/2004. Las oficinas de farmacia utilizarán la tarjeta sanitaria tanto para identificar al paciente como para acceder a la receta electrónica, artículo 8 y artículo 9 del Real Decreto 1718/2010.

12. Limitación: la limitación de datos e información en la tarjeta sanitaria no podrá ser impuesta por terceros a los responsables de tratarla. La tarjeta sanitaria está íntimamente vinculada con el derecho a la prestación de la Seguridad Social o al derecho a utilizar la Cartes de Servicios del Sistema Nacional de Salud.

    El derecho de limitación del tratamiento que reconoce el artículo 18 del Reglamento (UE) 2016/679, debe ser matizado pues puede chocar con artículo 6.1.c y 6.1.d. del Reglamento (UE) 2016/679.

    En el supuesto de que la persona quiera limitar el tratamiento de sus datos en su tarjeta sanitaria la Administración sanitaria debería ver si dicha limitación es posible.

    Aunque, no parece que haya pase legal que pueda impedir que la persona limitara el tratamiento de los datos de la tarjeta sanitaria al ámbito de la Administración sanitaria de la Comunidad Autónoma donde reside y en donde utiliza habitualmente los servicios asistenciales del Sistema Nacional de Salud.

13. Organización: la organización de los datos e información de la tarjeta sanitaria está regulada por el Anexo de Criterios básicos de las recetas médicas y órdenes de dispensación, del Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.

14. Recogida: la recogida de datos e información la hace la Administración sanitaria.

15. Registro: el registro del dato e información en la tarjea sanitaria corresponde a la Administración sanitaria.

16. Supresión: la supresión de datos implica su destrucción o eliminación por petición del titular de los datos.

    La supresión de los datos personales además de ser un elemento básico del tratamiento de datos está reconocida como derecho por el artículo 17 del Reglamento (UE) 2016/679 y por los concordante de la Ley 3/2018.

    Si bien no se puede renunciar a un derecho de la Seguridad Social, así reza el artículo 3 Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social, el suprimir los datos

[522] MS. Ministerio de Sanidad (2010). "Interoperabilidad plena de las tarjetas sanitarias" Disponible en https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/tic01.htm (31/01/2021).

personales de la tarjeta sanitara y en consecuencia de la Base de Datos de Población Protegida del Sistema Nacional de Salud, no significa renunciar al derecho de la prestación.

Aunque la tarjeta sanitaria Individual es un documento individual y personalizado que acredita el derecho a la asistencia sanitaria pública tanto del pensionista como de los beneficiarios, no es el único. El Certificado Provisional Sustitutorio (CPS) emitido por la Seguridad Social, también certifica el mismo derecho.

Cuando se ha visto el derecho a la supresión en cuanto a la historia clínica, se ha mencionado que este derecho está limitado por el criterio del médico responsable en base a que este puede entender que la información que se quiere eliminar puede ser necesaria para salud o seguridad del paciente o para la salud de terceras. Sin embargo, la supresión de los datos de la tarjeta sanitaria no pone en peligro la asistencia sanitaria de la persona, tan solo limitará a la persona el acceso a la financiación pública de la asistencia sanitaria que reciba.

El artículo 17 del Reglamento (UE) 2016/679 entiende que el interesado puede conseguir la supresión cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento. La supresión no será posible cuando el tratamiento de los datos sea necesario para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público, por razones de interés público en el ámbito de la salud pública.

Parece que la supresión de la tarjeta sanitaria no afecta a ninguna de las circunstancias que el artículo 17 expone para que no se puedan suprimir los datos de la tarjeta sanitaria. En el caso concreto de la tarjeta sanitaria se entiende que la oposición actuaría igual que supresión o la limitación.

17. Utilización: la utilización de tarjeta sanitara está ligada a la asistencia sanitaria del Sistema Nacional de Salud. No requerirá consentimiento de las personas en base al artículo 9.2.h) y también por el artículo 6.1.c) Reglamento (UE) 2016/769. También será utilizada por el personal de las oficinas de farmacia en base a los argumentos utilizados en el Acceso.

3.2.5.2. Elementos complementarios del tratamiento de la tarjeta sanitaria

En el capítulo 5.3.2 del Título I, se han tratado los elementos complementarios del tratamiento de datos. Si bien esta Tesis entiende a los elementos básicos del tratamiento de datos como a todas las operaciones y acciones incluidas en el artículo 4 del Reglamento (UE) 2016/679, por otra parte, también describe y define los elementos complementarios del tratamiento, como todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4.2), definiciones, del Reglamento (UE) 2016/679. Estos elementos complementarios son: acciones u operaciones previas al tratamiento

de los datos personales; o acciones u operaciones colaterales al tratamiento de datos; o que son acciones u operaciones necesarias para que este tratamiento sea lícito.

Estos elementos complementarios que aparecen en el Reglamento (UE) 2016/679 y/o la Ley Orgánica 3/2018 comprenden: el bloqueo; la circulación y portabilidad; el mantenimiento; la minimización; la exactitud de datos; rectificación; tráfico; y la transferencia y transmisión internacional. Con relación a la tarjeta sanitaria se obvian los siguientes elementos complementarios: la anonimización, la reidentificación, la reutilización y la seudonimización.

Elementos complementarios, en base al Reglamento (EU) 2016/679 y a la Ley 3/2018, aplicados a la tarjeta sanitaria constan, ordenado por orden alfabético, en el listado siguiente, a la derecha del texto consta la norma en la que el elemento está contemplado:

1. Bloqueo: el bloqueo de los datos consiste en la identificación y reserva de estos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, al igual que la anonimización, es incompatible con la naturaleza de la propia tarjeta sanitaria. — Ley Orgánica 3/2018

   Este tratamiento solo está en manos de la Administración sanitaria que gestiona las Bases de Datos de Población Protegida.

2. Exactitud: la exactitud en los datos de una tarjeta sanitaria es una condición fundamental en su registro. Le corresponde a la Administración sanitara atender a este tratamiento, artículo 5.2 del Real Decreto 1718/2010. Este elemento complementario del tratamiento es también un principio reconocido en el artículo 5.1.d) y artículo 18.1.a) del Reglamento (UE) 2016/679 — Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

3. Circulación: las tarjetas sanitarias son documentos personales que no se deben circular. Sin embargo, los datos de las tarjetas sanitarias registrados en las Bases de Datos de Población Protegida sí que pueden ser movilizados, de hecho, el fin de la Base de Datos es ser consultada y en consecuencia circular los datos en ella contenidos. — Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

4. Mantenimiento: mantenimiento y conservación son términos muy cercanos. El mantenimiento le corresponde a las Administraciones sanitarias competentes, artículo 5.2 del Real Decreto 1718/2010. El mantenimiento constará por una parte de la reposición de tarjetas sanitarias defectuosas y, por otra parte, el mantenimiento de la Bases de Datos de Población Protegida — Ley Orgánica 3/2018

5. Minimización: este tratamiento de datos no tiene sentido aplicado a la tarjeta sanitaria pues la estructura de datos está impuesta por la normativa. — Reglamento (UE) 2016/679

6. Portabilidad: en este caso se atiende a lo dicho para la circulación. La tarjeta sanitaria será portada por todos sus titulares en especial cuando acudan a un centro sanitario público en busca de atención y cuando acuda a la oficina de farmacia a adquirir el producto prescito. En este sentido, la portabilidad es una exigencia intrínseca a la naturaleza de la tarjeta sanitaria. — Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

7. Rectificación: la rectificación de la tarjeta sanitaria tan solo puede producirse por la Administración sanitaria, artículo 5.2 del Real Decreto 1718/2010. La rectificación de la tarjeta sanitaria corresponde a la misma categoría de administrativa que la rectificación de cualquier documento oficial o documento emitido por la Administración Pública. — Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

8. Tráfico: el tráfico de datos de la receta se remite a la circulación y a la portabilidad. En este supuesto, se entendería tráfico de una tarjeta sanitaria como la movilidad del documento entre distintas personas, lo cual no tiene sentido. — Ley Orgánica 3/2018

9. Transferencia: este supuesto se remite a lo mismo que lo dicho en el supuesto del tráfico. Se descarta la aplicación de la transferencia a la tarjeta sanitaria propiamente dicha, pero no se descarta en absoluto la transferencia de datos de la Bases de Datos de Población Protegida, ya tratado en el punto relativo a la circulación. — Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

10. Transmisión internacional: la transmisión de datos de la tarjeta sanitaria individual, no se contempla por el hecho de que existe una tarjeta sanitaria para este efecto dentro de la Unión Europea, esta es la tarjeta sanitaria europea[523]. Los datos de la Bases de Datos de Población Protegida no precisan de la transmisión internacional dado que a estos efectos ya existe la tarjeta sanitaria europea. — Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

3.2.5.3. Elementos adicionales en el tratamiento de la tarjeta sanitaria

En el capítulo 5. 3 del Título I, se han tratado los elementos adicionales en el tratamiento de datos. Si bien esta Tesis entiende a los elementos básicos del tratamiento de datos como a todas las operaciones y acciones incluidas en el artículo 4 del Reglamento (UE) 2016/679, por otra parte, también describe y define los elementos complementarios del

[523] *Vid. Supra p 292*, capítulo 1.2.5.3.2., del Título III.

tratamiento, como todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4.2), definiciones, del Reglamento (UE) 2016/679, entiende los elementos adicionales en el tratamiento de datos como las acciones u operaciones adicionales, que no son ni básicas ni complementarias, que se pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley orgánica 3/2018 o en alguno de estad dos normas.

Estos elementos adicionales que aparecen en el Reglamento (UE) 2016/679 y/o la Ley Orgánica 3/2018 comprenden: automatización, confidencialidad, consentimiento y oposición.

Elementos adicionales, en base al Reglamento (EU) 2016/679 y a la Ley 3/2018, aplicados a la tarjeta sanitaria constan (ordenado por orden alfabético) en el listado siguiente, a la derecha del texto consta la norma en la que el elemento está contemplado:

1. automatización: el Reglamento (UE) 2016/679 al referirse a tratamiento automatizado se refiere al que tiene soporte informático y lo diferencia del tratamiento manual. Lo relaciona con la elaboración de perfiles. Aun así, el Reglamento (UE) 2016/679 dice en su Considerando 15: "A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas". Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   En este orden de cosas, la automatización de la tarjeta sanitaria se refiere a su utilización en red o en las oficinas de farmacia.

   Los criterios de la automatización de la tarjeta sanitaria son aplicables a la receta electrónica y a la obtención electrónica de la historia clínica.

2. Confidencialidad: si bien la confidencialidad no es un tratamiento, si es una forma de realizarlo, es decir, un tratamiento confidencial. Esta forma de tratar los datos se establece como un deber en el artículo 15 de la Ley 3/2018 y del artículo 5 del Reglamento (UE) 2016/679. Tal como dice el artículo 15.2 de la Ley 3/2018, el deber de confidencialidad será complementario al deber de secreto profesional. Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

   El tratamiento confidencial es relativo al principio de intimidad y reserva de la información y datos que contiene la tarjeta sanitaria y en especial a los Códigos que dan acceso a la historia clínica del paciente, en su totalidad o en parte. De tal forma que el personal sanitario tiene el deber de garantizar la confidencialidad y la intimidad

de los pacientes cuando utilicen la tarjea sanitaria de cualquier persona, artículo 111.2.b). 19ª. Real Decreto Legislativo 1/2015.

El tratamiento de los datos de la tarjeta sanitaria, electrónica o en modo manual, deberá ser siempre realizado respetando la máxima confidencialidad, artículo 19 del Real Decreto 1718/2010, reserva o secreto.

3. Consentimiento: el consentimiento para acceder a los datos de una persona es una condición general que impone el Reglamento (UE) 2016/679, sean de la naturaleza que sean, es el artículo 6 del Reglamento (UE) 2016/679 el que impone las bases jurídicas. Estas condiciones de licitud del artículo 6 se extreman en los supuestos del artículo 9 del Reglamento (UE) 2016/679 al especificar el tratamiento de categorías especiales de datos personales, entre los que incluye cualquier dato relativo a la salud de una persona.

Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y Ley 41/2002

El registro y acceso a los datos de la tarjeta sanitaria clínica deberá estar sujeto en algún momento al consentimiento de la persona y a la información por parte del responsable del tratamiento de los tratamientos a los que se puede someter dichos datos.

Sin embargo, a través del artículo 9 del Reglamento (UE) 2016/679, en su apartado 2.h) y a través del artículo 6 del Reglamento (UE) 2016/679 en su apartado 1.c), podría entenderse que el consentimiento para el tratamiento de los datos de la tarjeta sanitaria no debería ser exigido en todos los casos.

Sin embargo, ambos artículos actúan como “cláusulas comodín”, es decir, artículo 6.1.c) y 9.2.h), hacen referencia al tratamiento en el sentido de la definición que el Reglamento (UE) 2016/679 hace en el artículo 4.2, lo cual no implica que sea de aplicación a todos y cada uno de los 11 elementos básicos de tratamiento o a los 11 elementos complementarios que conlleva el tratamiento de datos.

Estas “cláusulas comodín”, deben ser tenidas en cuenta en el contexto del Reglamento (UE) 2016/679 cuyo objeto (artículo 1) es establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales.

Un análisis del contenido de estas “cláusulas comodín” tiene como fin hacer coherente y posible la protección de la persona pretendida por el Reglamento (UE), para que una hipotética protección llevada a sus extremos pudiera impedir la protección de otros bienes jurídicos de igual o superior consideración.

En este orden de cosas, los elementos básicos del tratamiento de datos de recogida y registro, junto con los elementos complementarios de exactitud, entre otros, no podrán llevarse a cabo sin la participación activa de la persona titular de los datos y que, sin la colaboración activa de la misma, no sería posible.

Así pues, independientemente de que las "clausulas comodín" pueden omitir el consentimiento de la persona para muchos elementos básicos y complementarios del tratamiento de los datos de la tarjeta sanitara, nada impide entender que el consentimiento, como acto de legitimación del tratamiento de datos personales, debe ser dato por la persona en el proceso de recogida y registro de la tarjeta sanitaria.

En todo caso, en el supuesto de que la Autoridad de control entendiera que este consentimiento no es necesario, se entiende que es inexcusable la aplicación del artículo 12 (Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado) del Reglamento (UE) 2016/679 así dice:

> "El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios".

Para concluir, el Considerando 61 del Reglamento (UE) 2016/679 dice que se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos.

4. Oposición: el derecho oposición al tratamiento de los datos está reconocido por el artículo 21 del Reglamento (UE) 2016/679 y por los concordantes de la Ley Orgánica 3/2018.

Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

Cuando se ha visto el derecho a la supresión en cuanto a la historia clínica, se ha mencionado que este derecho está limitado por el criterio del médico responsable. También se ha visto que la oposición a los datos en la receta no tiene sentido. Sin embargo, la oposición al tratamiento de los datos de la tarjeta sanitaria no pone en peligro la asistencia sanitaria de la persona, tan solo limitará a la persona el acceso a la financiación pública de la asistencia sanitaria que reciba.

Incluso, el artículo 21 del Reglamento (UE) 2016/679 entiende que el interesado se puede oponer aun cuando se alegue el artículo 6.1.e) y el artículo 6.1.f) salvo que se acrediten motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

En el caso concreto de la tarjeta sanitaria se entiende que la oposición actuaría igual que supresión o la limitación.

3.2.5.4. Otros elementos del tratamiento de la tarjeta sanitaria distintos de los encontrados en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018

Otras normas con rango de Ley y otras con rango de Decreto introducen además otros de los elementos del tratamiento de la tarjeta sanitaria, estos son la cesión, custodia y emisión.

1. Cesión: se remite a lo dicho en cuanto a la comunicación por transmisión. Real Decreto 183/2004

   Con criterio general la cesión de datos personales no está autorizada salvo consentimiento del interesado o salvo lo que las "cláusulas comodín" permitan excepcionar.

   En todo caso el Consejo Interterritorial del Sistema Nacional de Salud o la Administración sanitaria competente debería consultar sobre la licitud de la cesión de datos a la Autoridad de control, artículo 7 del Real Decreto 183/2004.

2. Custodia: la custodia de cada tarjeta sanitaria Individual le corresponde a la persona o a sus representantes legales. Real Decreto 183/2004

   En cuanto a la Base de Datos de la Población protegida la custodia le corresponde a las Administraciones sanitarias emisoras de la tarjeta sanitaria individual, artículo 5.3 del Real Decreto 183/2004.

3. Emisión: las Administraciones Públicas sanitarias autonómicas y el Instituto Nacional de Gestión Sanitaria emitirán una tarjeta sanitaria individual con soporte informático a las personas residentes en su ámbito territorial que tengan acreditado el derecho a la asistencia sanitaria pública, artículo 2.1 del Real Decreto 183/2004. Real Decreto 183/2004

3.3. Tratamiento de datos de la investigación en salud (disposición adicional decimoséptima y disposición final quinta de la Ley Orgánica 3 /2018)

En el apartado 2 del capítulo 3 del Título III, ha planteado el análisis del tratamiento en datos en base a los tres soportes principales del dato relativo a la salud, estos son, la historia clínica, la receta y la tarjeta sanitaria.

En este punto 3 del capítulo 3 del Título III, se pretende concretar el tratamiento de los datos de las personas en los procesos o en los escenarios de investigación de la salud, de forma distinta de la utilizada en el anterior análisis, dado que al hablar de investigación en la salud no hablamos de soportes materiales o conceptuales, sino que nos referimos a una actividad, a la actividad científica.

La naturaleza de lo que se pretende analizar, la actividad científica en el sector de la salud, obliga a acudir directamente a dos disposiciones de la Ley Orgánica 3/2018, por una parte, a la Disposición adicional decimoséptima y, por otra parte, a la Disposición final quinta.

El preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, menciona que el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Permitiendo, además, dejar a salvo las distintas habilitaciones legales existentes antes de su aprobación, tal y como se indica en la Disposición adicional decimoséptima, respecto de la legislación sanitaria y aseguradora.

La Disposición adicional decimoséptima de la Ley Orgánica 3/2018, en su punto 2, introduce dos concetos nuevos, la seudonimización y al reidentificación.

El Reglamento (UE) 2016/679, en su artículo 4, define seudonimización como:

> "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable."

La seudonimización, en este contexto, debe entender como un proceso para procurar la licitud. Así pues, la licitud de la utilización de datos personales con fines de investigación en salud pública y/o biomedicina se produce a través del tratamiento de datos personales mediante la acción de la seudonimización. Sin embargo, para que se perfeccione el proceso de licitud deberán cumplirse cuatro condiciones adicionales:

1. Primera condición: independencia entre el equipo investigador y la persona que realice el proceso de seudonimización y el de reidentificación, mediante una separación técnica y funcional.
2. Segunda condición: compromiso expreso de confidencialidad.
3. Tercera condición: recusación de cualquier actividad de reidentificación futura.
4. Cuarta condición: preventivamente, se adoptarán suficientes medidas de seguridad para evitar tanto la reidentificación como el acceso de terceras personas no autorizadas.

La reidentificación en el nuevo ordenamiento jurídico de protección de datos personales no está autorizada. Sin embargo, la Ley Orgánica 3/2018 autoriza expresamente la reidentificación de los datos en un solo caso.

Esta excepción de la Ley Orgánica 3/2018 se activa cuando se manejen datos seudonimizados, en un proceso de investigación de la salud, y se detecte algún tipo de riesgo o peligro. Este peligro puede ser tanto el que ponga en riesgo la integridad física de una persona o grupo de personas, como el que atente contra los derechos de las personas protegidas por esta ley o cuando se deba garantizar la atención médica.

Dentro de la excepción, se deben incluir aquellas que afectan a los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679, en un proceso de investigación de la salud, cuando:

1. Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.
2. El ejercicio de tales derechos se refiera a los resultados de la investigación.
3. La investigación tenga por objeto un "interés público esencial" relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

En una investigación en salud pública y biomédica, en base al punto 2 de la Disposición adicional decimoséptima de la Ley Orgánica 3/2018, y conforme a las garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, se procederá a:

a) Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la Autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.
b) Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.
c) Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.
d) Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

El papel de los comités de ética viene regulado en la Disposición adicional decimoséptima. El uso de datos personales seudonimizados deberá contar con un informe del comité de ética de la investigación previsto en la normativa sectorial. Si no se dispone de comité de ética se requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto en la materia.

Los comités de ética de la investigación en el ámbito de la salud en el sentido amplio de término, antes del día 6 de diciembre de 2019, deberán contar con un delegado de protección de datos o de un experto en el RGPD cuando se pretenda el tratamiento de datos personales o de datos seudonimizados o anonimizados.

3.4. Base jurídica para el tratamiento de los datos relativos a la salud

El espíritu y la esencia del RGPD y de la Ley Orgánica 3/2018 es la máxima protección de los derechos a la intimidad de las personas, en lo que respecta a sus datos personales, dentro del escenario de liberad de circulación de personas de la Unión Europea, mediante la autorización de determinados tratamientos de datos, con la ayuda de un número importante de excepciones, y mediante la legitimación de las personas que pueden realizar dichos tratamientos autorizados en función de base jurídica[524].

El Reglamento (UE) determina que tan solo determinadas personas o profesionales podrán tratar los datos personales relativos a la salud de las personas, acogiéndose al tratamiento de las categorías especiales de datos a que se refiere el apartado 2, letra i), en los relativos a la salud, del artículo 9. Esta es la base jurídica que legitima a las personas al tratamiento de estos datos y que ha sido denominada en el capítulo 5.5. como legitimación subjetiva indirecta o legitimación subjetiva a terceros[525].

Estas personas autorizadas por el Reglamento (UE), de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, son:

1. los profesionales sujetos a la obligación de secreto profesional, o bajo su responsabilidad,
2. cualquier otra persona sujeta también a la obligación de secreto.

La elección por parte del Reglamento (UE) 2016/679 de esta solución general, el secreto profesional, inicialmente parece escrupulosa y muy acertada, pero en la medida que se analiza el concepto de secreto profesional cabe deducir que se comporta casi como una "cláusula comodín" o como la cláusula que excluye la misma regla que crea, cláusulas habítales en el texto del RGPD.

Se entiende por secreto profesional la obligación que adquieren unos determinados profesionales de no desvelar ningún tipo de información que haya podido suministrale un cliente suyo.

Este deber de confidencialidad nace de la propia naturaleza del servicio que recibe el cliente por arte del profesional y que, sin esta condición, confidencialidad, el servicio no sería posible llevarlo a cabo, es decir, sería incompatible con la naturaleza y esencia del servicio.

La naturaleza del servicio que obliga al deber de confidencialidad puede venir atribuida por preceptos legales de obligado cumplimiento, como es el caso de un abogado y su cliente o el caso de un paciente y su médico o cualquier profesión de la salud, como enfermería, psicología, farmacia, etc.. En el caso del abogado y cliente esta confidencialidad viene establecida tanto por el artículo 24 de la Constitución como por el artículo 542.3 de la Ley Orgánica 6/1985, del Poder Judicial. En el caso de os

[524] *Vid. Supra p 145*, capítulo 5.5., del Título I.
[525] *Vid. Supra p 150*, capítulo 5.5.3., del Título I.

profesionales sanitarios la atribución de confidencialidad viene comandada por la relación de la información suministrada con la protección de determinados derechos fundamentales de la persona como es el de la intimidad, artículo 18 de la Constitución Española de 1978, y dignidad entre otras. El secreto profesional también se aplica a profesiones como los delegados de prevención de accidentes laborales, y el trabajador social, en alguna forma también se aplica al periodista, artículo 10 del Código Deontológico de la Federación de Asociaciones de Periodistas de España y artículo 19 de la Declaración Universal de Derechos Humanos.

El deber de secreto profesional se extiende, a modo de mancha de aceite, al ámbito de trabajo y relaciones laborales del profesional directamente implicado en el mismo, así, en el caso de los abogados, artículo 5 del Código Deontológico adoptado por el Estatuto General de la Abogacía Española, aprobado por Real Decreto 658/2001, de 22 de junio, se extiende a los pasantes, procuradores, licenciados en derechos o meros estudiantes de derecho en prácticas y cualquier personal auxiliar con acceso a los datos del cliente, como también en el caso de los profesionales sanitarios, se extiende al personal que accede a los datos de historia clínica en ejercicio de sus funciones, artículo 16.6 Ley 41/2002.

Muy vinculado con lo dicho en el párrafo anterior, el ordenamiento jurídico también crea la figura del "*secreto profesional sobrevenido*"[526], aunque no de forma explica si de forma implícita y clara, a su vez. Este tipo de secreto profesional es el que viene atribuido por las circunstancias de su trabajo o desempeño laboral, atemporales.

Este tipo de secreto profesional sobrevenido es el que nace en un profesional o trabajador que, por circunstancias de su trabajo o desempeño laboral, haya tenido acceso a ciertos documentos confidenciales de algún tipo de persona, de tal forma que por haber tenido acceso a datos especialmente protegidos de una persona en el ejercicio de sus funciones queda sujeto al deber de secreto. Es decir, es un deber sobrevenido porque antes de tener acceso a dichos documentos su profesión o funciones no estaban sujetas al deber de secreto profesional, sino que es después de acceder a estos datos protegidos cuando nace dicha obligación.

Este deber de "secreto profesional sobrevenido" queda reflejado en las siguientes disposiciones: el artículo 199 del Código Penal; el artículo 127 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras; el artículo 10 de la Ley 14/1986, de 14 de abril, General de Sanidad; el artículo 16.6 de La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; el artículo 5 de la Ley 14/2007, de 3 de julio, de Investigación biomédica; y el artículo 43 de la Ley 33/2011, de 4 de octubre, General de Salud Pública.

Ahora bien, el secreto profesional, en cualquiera de sus variantes, no es una cuestión absoluta. La fundamentación del secreto profesional se debe contraponer a la obligación de poner en conocimiento de la autoridad competente cualquier tipo de delito público,

[526] *Vid. Supra p 150,* capítulo 5.5.3., del Título I.

la cual tiene algunas excepciones aplicables solo a los abogados y los que ejercen funciones eclesiásticas o son ministros de cualquier religión.

En este orden de cosas, tal como se ha visto con anterioridad si bien es cierto que tienen obligación de secreto profesional en primer lugar los abogados y, en segundo lugar, los profesionales de la salud, los delegados de prevención de accidentes laborales, el trabajador social y en alguna forma los periodistas, también es cierto que por otra parte tienen la obligación de denunciar el conocimiento o notica sobre un acto delictivo toda persona que por el cargo que ocupa tuviere noticas de un delito y tienen el deber de denunciar el que tuviere conocimiento o alguna notica de un delito. Sin embargo, esta obligación tampoco es absoluta y tiene, a su vez, una serie de excepciones.

A esta obligación del deber de denunciar se opone una serie de exclusiones, así pues, no tienen el deber de denunciar, las siguientes personas: los menores de edad, los incapaces, los cónyuges (no separados legalmente) o con análoga relación de afectividad, los ascendientes y descendientes hasta segundo grado de parentesco, los abogados y procuradores por la información que reciban de sus clientes y los eclesiásticos y ministros de culto disidentes, de las noticias que tuvieran en conocimiento por medio del ejercicio de sus funciones.

Se esta forma la licitud del tratamiento de los datos relativos a la salud protegido por el artículo 9, cuando el interesado no haya hechos manifiestamente públicos estos datos, corresponde a personas en uno de estos supuestos o bases jurídicas:

1. Que estén en poder del consentimiento explícito para el tratamiento de dichos datos personales no existiendo prohibición de dicho consentimiento, lo cual no exime de secreto profesional.
2. En actividad clínica o asistencial o relativa a la salud, sujetas a la obligación de secreto profesional, sin necesidad de consentimiento del interesado.
3. Obligadas al tratamiento de tales datos cuando sean necesarios para, lo cual no exime de secreto profesional, pero si exime de consentimiento:
    a. el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado, en el ámbito del derecho laboral y de la seguridad y protección social,
    b. proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento,
    c. la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial,
    d. razones de un interés público esencial,
    e. razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios,

f. con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

De esta forma se observa que para el tratamiento de los datos protegidos por el artículo 9, el consentimiento del interesado tiene excepciones en los siguientes entornos, legitimando, en su caso, a quien está obligado al tratamiento de datos personales:

1. en el ámbito del derecho laboral y de la seguridad y protección social,
2. en el supuesto de que el interesado no esté capacitado, física o jurídicamente,
3. en los tribunales actúen en ejercicio de su función judicial,
4. en el interés público esencial,
5. en entornos asistenciales, médicos o clínicos,
6. en salud pública,
7. en el ámbito de la investigación científica o histórica o fines estadísticos.

A todo esto, cabe añadir que el artículo 6.1 del Reglamento (EU) 2016/679 legitima el tratamiento de datos en las determinadas circunstancias, se entiende siempre y cuando su tratamiento no esté prohibido por el artículo 9 del Reglamento (EU) 2016/679 o estando prohibido se le aplique el apartado 2 del mismo artículo, que es el que levanta la prohibición del apartado 1.

De esta forma están autorizados por el RGPD para tratar los datos relativos a artículo 9.2. del Reglamento (EU) 2016/679, los que estén obligados al secreto profesional cuando el ámbito es el de la asistencia o clínico o médico, o las personas que estén en una de las siguientes situaciones, en base al artículo 6.1 del Reglamento (EU) 2016/679:

a. “poseer el consentimiento del interesado
b. tener que ejecutar un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales
c. para cumplir una obligación legal del responsable del tratamiento
d. para proteger intereses vitales del interesado o de otra persona física
e. para una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento
f. 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. “

Lo cual significa que, si hubiera algún tratamiento de datos relativos a la salud, artículo 9.1, que no se acogiera a alguna exclusión del artículo 9.2, no se podría aplicar el artículo 6.1 de legitimación para el tratamiento, y no nadie estaría autorizado para tratarlo.

Por último, este es el supuesto de los datos personales relativos a la salud de una persona que no son necesarios para el mantenimiento de su salud, como por ejemplo hacer referencia a datos sobre una enfermedad del pasado de la persona afectada y ya

resuelta, cuestión muy frecuente en los datos de las historias clínicas de los pacientes o usuarios de la sanidad pública o privada. Se entiende todo ello, siempre que estas historias clínicas no estén inmersas en procesos de investigación biomédica o estadística, previsto en el punto f) del apartado 2 del artículo 9 o en la Disposición adicional séptima de la Ley orgánica 3/2018, relativa a procesos de seudonimización en procesos de investigación biomédica.

3.4.1. Base jurídica para el tratamiento de la historia clínica

Los centros sanitarios son organizaciones de trabajo de alta complejidad, en donde se presta un servicio a las personas que requieren atención de su salud o atención a aspectos relativos a su salud, estén o no estén enfermas.

Estos servicios de asistencia sanitaria están compuestos de muchas tareas, procesos y procedimientos llevados a cabo por profesionales y trabajadores de diversas disciplinas a través de un complejo engranaje. De esta forma, la ley 41/2002, en su artículo 16.4 prevé que además del facultativo o profesional de la salud, el personal de administración y gestión de los centros sanitarios puede acceder a los datos de la historia clínica, aunque estos solo podrán acceder a los datos relacionados con sus propias funciones.

En los centros sanitarios no tan solo actúan y tienen acceso los profesionales y trabajadores contratados por estos mismos centros, sino que también actúan otros profesionales, sanitarios y no sanitarios, pertenecientes al sistema sanitario ajenos al centro sanitario en donde se presta el servicio. En este orden de cosas, el artículo 16.5 de la Ley 41/2002 autoriza y prevé que

> "El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria."

La posibilidad de acceder al tratamiento de datos de categorías especiales de forma legítima la establece el Reglamento (UE) en el artículo 9.3. determina:

> "Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes."

Así pues, es el secreto profesional lo que determina quién pueda y no quién no puede tratar datos personales de categorías especiales sin vulnerar su licitud.

Tal como ya hemos adelantado en el punto anterior a este y en el Capítulo 5.5 del Título I "Legitimación para el tratamiento de los datos del artículo 9 del Reglamento (UE)" hay dos tipos de secreto profesional.

El primer tipo de secreto profesional es aquel que viene definido expresamente por el ordenamiento jurídico y está vinculado a una profesión y a una actividad profesional.

El segundo tipo de secreto profesional es aquel que se genera por la actividad de una persona en un momento dado y que en la Tesis se denomina Secreto Profesional Sobrevenido. Es decir, aquella persona que, no estando obligada a guardar secreto con carácter general, adquiere esta obligación después de tener acceso a un determinado tipo de datos. Tal es lo que ocurre con lo previsto en el artículo 16.6 de la Ley 41/2002, al afirmar: "El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto".

El tratamiento, acceso, a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, artículo 16.3 de la Ley 41/2002.

El acceso a la historia clínica con fines no asistenciales, en base al artículo 16 de la Ley 41/2002, obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales. Asimismo, se exceptúan los supuestos que dispongan los jueces y tribunales en procesos correspondientes. Por último, con carácter general el acceso a los datos y documentos de la historia clínica queda limitado, estrictamente, a los fines específicos de cada caso, artículo 16.3 de la Ley 41/2002.

Sin embargo, cuando sea necesario acceder a datos de la historia clínica para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública, artículo 16.3 de la Ley 41/2002.

El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos, artículo 16.3 de la Ley 41/2002.

Por último y a modo de conclusión, el tratamiento de datos relativos a la salud que no se acoja a alguna exclusión del artículo 9.2, no podrá utilizar los criterios del artículo 6.1 para la licitud del tratamiento. Por otra parte, no hay licitud para el tratamiento de los datos de las historias clínicas en archivos pasivos o datos en las historias clínicas no necesarios para atender a la salud actual de la persona, ni para atender cuestiones de salud pública, ni útiles para procesos de investigación o que estén fuera de estos procesos.

3.4.2. Base jurídica para el tratamiento de las recetas

La receta[527], es un documento con datos personales que se somete al tratamiento de daros personales de categorías especiales del artículo 9 del Reglamento (UE).

El tratamiento se autoriza por el artículo 9 del Reglamento (UE) 2016/679, en letra b) del punto 2, al decir que la prohibición del punto uno no se aplica en el caso: en su punto h), cuando dice: el tratamiento es necesario para fines de ….., prestación de asistencia o tratamiento de tipo sanitario o social, …...;

En este orden de cosas, la licitud vendría condicionada por la aplicación el artículo 9.3 del Reglamento (UE) cando dice:

> "Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes."

En cuanto a la legitimación del médico, no hay duda pues se aplica los mismos criterios y fundamentos que en el caso de la historia clínica[528]. Con carácter general en los centros sanitarios la receta no debería ser tratado por otro personal distinto del médico o enfermería.

La peculiaridad de este tipo de documento es el amplio elenco de profesionales o personas que puedan llegar a tratar sus datos. El más importante de este grupo de profesionales es el farmacéutico de la oficina de farmacia o del servicio de farmacia hospitalario.

El tratamiento de los datos en la oficina de dispensación o farmacia puede ser realizados por personas que no sean el profesional con deber de secreto profesional. En este caso, el secreto profesional sería el sobrevenido, visto y descrito en el capítulo 5.5. del Título I.

El secreto profesional del farmacéutico de oficina de farmacia además de estar regulado por las disposiciones generales a todo el secreto profesional viene establecido[529] en el siguiente ordenamiento: n

> "El secreto profesional siempre ha sido tutelado por los farmacéuticos de oficina, y venía exigido por la Ley General de Sanidad y por el Código Penal, que en su artículo 199 tipifica como delito «revelar secretos ajenos de los que se tenga conocimiento por razón de oficio». La Ley del Medicamento, en su artículo 108, califica como falta grave «el incumplimiento por parte del personal sanitario del deber de garantizar la

[527] *Vid. Supra p 275,* capítulo 1.2.5.2., del Título III.
[528] *Vid. Supra p 268,* ,capítulo 1.2.5., del Título III.
[529] CORDONES A. (2002) "Protección de datos de carácter personal en la oficina de farmacia". OFFARM, 21 (1), 112-117. Disponible en https://www.elsevier.es/es-revista-offarm-4-articulo-proteccion- datos-caracter-personal-oficina-13025054. (30/04/2021). p 112.

> confidencialidad y la intimidad de los pacientes en la tramitación de las recetas y órdenes médicas». El artículo 109 de la misma Ley establece las sanciones procedentes a los que cometan infracciones en este ámbito."

Por otra parte, la licitud para el farmacéutico y el personal especializado que trabaje en las oficinas de farmacia se puede basar a través del artículo 9.2, el que exceptúa la prohibición del tratamiento de este tipo de datos, en su punto h) entiende que no hace falta el consentimiento de la persona. El artículo 9.2.h), dice que no se aplica la prohibición del tratamiento de este tipo de datos cuando: "h) el tratamiento es necesario para fines …., prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, …..".

El artículo 10.8 de Ley 19/1998, de 25 de noviembre, de Ordenación y Atención Farmacéutica de la Comunidad de Madrid, dice: "El Farmacéutico en su ejercicio profesional está obligado al secreto y confidencialidad que se derive del mismo."

Diversas Comunidades Autónomas utilizan expresiones parecidas en sus leyes de ordenación farmacéutica, como, por ejemplo, el artículo10.1.d) de la Ley 13/2001, de 20 diciembre 2001, Ordenación Farmacéutica de la Comunidad de Castilla León, dice:

> "d) A la confidencialidad de todos los datos personales que se encuentren a disposición de los establecimientos y servicios farmacéuticos, y en particular de los referentes a su estado de salud y medicamentos que le hayan sido prescritos y dispensados, salvo los de interés sanitario en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."

El artículo 6.4 del Código de Deontología de la Profesión Farmacéutica del Consejo General de Farmacéuticos, dice: "El secreto profesional es inherente al ejercicio de la profesión farmacéutica y el farmacéutico está obligado a salvaguardar la intimidad del paciente/usuario".

En resumen. Tendrán acceso a la receta del paciente en base al artículo 9 del Reglamento (UE) 2016/679 cualquier profesional sujeto a la obligación de secreto profesional. Tendrá legitimidad para el acceso a los datos de la receta bien por el artículo 9 del Reglamento (UE) 2016/679 o bien por los prescriptores a los que se refiera el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios. De esta forma se hace referencia al enfermero y fisioterapeutas prescriptores, podólogo, el farmacéutico o personal auxiliar y el médico que le haya recetado y el profesional sanitario sanitarios que por exigencias de su puesto de trabajo y función asistencial tenga la necesidad de conocer el contenido de la receta[530].

3.4.3. Base jurídica para el tratamiento de la tarjeta sanitaria

En base a la consideración sobre si los datos de la tarjeta sanitaria son datos personales o son de carácter personal o si estos son datos se deben considerar datos relativos a la

[530] *Vid. Supra p 341,* capítulo. 3.2.4., del Título III.

salud pues su tratamiento nace y es específico del sistema de salud. Además, son datos automatizados que permiten el acceso a datos relativos a salud en sentido estricto.

En este sentido el Considerando 35 del Reglamento (UE) 2016/679 dice:

> "Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro."

En base a este Considerando 35, se debe entender que los datos que constan en la tarjeta sanitaria deben ser considerados datos personales relativos a la salud. Sin embargo, también hay que tener en cuenta que el tratamiento de la tarjeta sanitaria puede darse en escenarios de trabajo muy distintos y, en consecuencia, a cada escenario le corresponderá un tipo de tratamiento. Unos escenarios no tienen posibilidad de conectar la tarjeta sanitaria con las bases de datos de las cuales es parte, y en otros escenarios la conexión es posible. Así pues, en un escenario, el tratamiento se entenderá como tratamiento de datos personales, del artículo 6 del Reglamento (UE), y el otro escenario, el tratamiento como categorías especiales de datos, del artículo 9 del Reglamento (UE).

La licitud del tratamiento de datos personales viene dada cuando se cumplan una de estas bases jurídicas, artículo 6 Reglamento 2016/679:

1. Por consentimiento.
2. Por exigencia legal, por contrato o por ley.
3. Por interés vitales de cualquier persona física.
4. Por interés público.
5. Por ejercicio de la autoridad pública.
6. Por el interés legítimo del responsable del tratamiento.

Por otra parte, la Agencia Española de Protección de Datos, en el mes de diciembre, ha publicado la "Guía para pacientes y usuarios de la sanidad". Esta guía en su página 6 publica el punto 2. "Legitimación para el tratamiento de datos de salud" y dice:

> "No es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para la recogida y utilización de datos personales y de salud si se van a utilizar para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del

> trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social. (La base de legitimación para este tratamiento de datos está establecida en el artículo 6.1.b) del RGPD para las entidades aseguradoras de salud privadas, y en el artículo 6.1.c) del mismo Reglamento para la sanidad pública)."

Si bien el doctorando entiende que las afirmaciones de la Agencia Española de Protección de Datos AEPD están faltas de fundamentación, lo cierto es que también es cierto que la AEPD abre el camino para aplicar las vías para la licitud del tratamiento de datos personales del artículo 6 del Reglamento (UE).

La AEPD utiliza los siguientes preceptos del Reglamento (UE):

> "Artículo 6. Licitud del tratamiento
>
> 1.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".

El artículo 6.1.b) lo utiliza para su aplicación a la sanidad privada y el artículo 6.1.c) lo utiliza para la aplicación a la sanidad pública.

En este orden de cosas, y en base a la tesis de la AEPD puede entenderse que el tratamiento de los datos de la tarjeta sanitaria podría ser licito sin consentimiento del interesado, por aplicación del artículo 6.1.c), es decir, "c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento." Lo cual no exclusa que dos obligaciones. La primera, en el momento en que la Administración pública o la Entidad Aseguradora privada, cree o edite la tarjeta sanitaria deberá contar con el consentimiento por escrito del interesado una vez que sea informado del uso que se hará de su tarjeta sanitaria y de las situaciones en las cuales se usará la tarjeta sanitaria con su consentimiento. La segunda, la persona interesada será informada de también de todos los derechos personales que tiene sobre sus datos y la forma de ejercitar cada uno de ellos en el escenario en donde se encuentre, en base al Capítulo III, de derechos del interesado, del Reglamento (UE) 2016/679 y al Título III, derechos de las personas, de la Ley Orgánica 3/2018.

Por otra parte, si el dato de la tarjeta sanitaria se entiende como vinculado al artículo 9 del Reglamento (UE) y debe someterse a los criterios del tratamiento de categorías especiales de datos personales, entonces las bases jurídicas de licitud son otras.

En este último supuesto, categorías especiales de datos, en base a la línea de argumentación de la AEPD, es posible entender que el artículo 9.2, el que exceptúa la prohibición del tratamiento de este tipo de datos, en su punto h) entiende que no hace

falta el consentimiento de la persona. El artículo 9.2.h), dice que no se aplica la prohibición del tratamiento de este tipo de datos cuando:

> "h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3."

Si la decisión es aplicar lo mencionado en relación al artículo 9.2.h), no es excusa para no exigir el otorgamiento del consentimiento en el momento de la emisión de la tarjeta sanitaria ni de la obligación del responsable del tratamiento de informar a la persona de todos los derechos que le ampara el Capítulo III, de derechos del interesado, del Reglamento (UE) 2016/679 y el Título III, de derechos de las personas, de la Ley Orgánica 3/2018 y la forma de ejercerlos en el ámbito de utilización de la tarjeta sanitaria. A lo cual se podría añadir, la obligación del centro sanitario de informar a la persona interesada, cada vez que utilizara su tarjeta sanitaria, por ejemplo, para activar su historia clínica, del tipo de uso que se está haciendo o que se va hacer de la misma.

EL Sr. D. José Antonio Prego de Oliver Fernández, en su Tesis Doctoral de 2017, afirma al respecto[531]:

> "La obligación de informar a los interesados cuanto se van a recabar, tratar o almacenar sus datos personales ya estaba recogida en la Directiva 95/46/CE. Sin embargo, el nuevo Reglamento General de Protección de Datos (RGPD) concede una mayor importancia a la información que se debe proporcionar a los ciudadanos cuyos datos van a tratarse, y contempla una lista exhaustiva de los contenidos que deben ser expuestos. Esta obligación debe estar en consonancia con otro importante mandato: el de informar de forma concisa, inteligible y con un lenguaje claro y sencillo."

En cuanto a las personas que puedan utilizar este tipo de documento, se aplica lo mismo que en el caso de la historia clínica. El acceso a la tarjeta sanitaria habrá de realizarse en base la normativa aplicable a la historia clínica del artículo 16 de la Ley 41/2002, en sus puntos 4. 5 y 6. El artículo 16 de la Ley 41/2002 dice:

> "4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.
>
> 5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

[531] PREGO DE OLIVER FERNÁNDEZ, JA. (2017) "La transparencia como elemento de apoyo al consentimiento en materia de Protección de Datos", Tesis Doctoral, Facultad de Derecho, Universidad Carlos III de Madrid, Getafe, España. Disponible en https://e-archivo.uc3m.es/bitstream/handle/ 10016/26447/tesis-juanantonio-prego-de-oliver-fernandez-2017.pdf?sequence=1&isAllowed=y. (30/04/2021). p 529.

> 6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto"

A su vez, es de aplicación el artículo 9.3 del Reglamento (UE) cando dice:

> "Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes."

Resumiendo, en primer lugar, la tarjeta sanitaria contiene datos personales que en función del escenario en el cual se utilice le es de aplicación el artículo 9 del Reglamento (UE). En segundo lugar, podrá hacer uso de la tarjeta sanitaria el profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, el personal de administración y gestión de los centros sanitarios en uso de sus funciones.

En tercer lugar, se entiende que, en todo caso, la persona interesada o titular del derecho, o su representante, deberá dar su Consentimiento en el momento que al Administración pública o la entidad de aseguramiento privada cree o emita la tarjeta sanitaria

En cuarto lugar, la persona interesada deberá ser informada, así mismo, en el escenario de un centro sanitario en donde sea atendida, en cada momento, del uso que se hace de su tarjeta sanitaria.

En quinto y último lugar, la persona titular del derecho o su representante al firmar el consentimiento o al ser informada de todo lo relativo al uso de la tarjeta sanitaria, será también informada de todos los derechos personales que tiene sobre sus datos y la forma de ejercitar cada uno de ellos en el escenario en donde se encuentre.

3.4.4. Base jurídica para el tratamiento de los datos para la investigación en salud

El Reglamento (UE) 2016/679 no afecta a las investigaciones en salud cuando los datos son anónimos. El artículo 89 del Reglamento (UE) 2016/679 relativo a las garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados.

La licitud para el tratamiento de los datos para la investigación en salud viene dada en primer lugar, por el consentimiento de la persona titular de los mismos y, en segundo lugar, en ausencia del consentimiento por garantías suficientes de confidencialidad.

Cuando no existe dicho consentimiento la legitimación vendrá dada, en los procesos de investigación biomédica, cuando los datos personales estén seudonimizados debiendo existir, a su vez, una clara independencia y neta separación entre los investigadores y

quienes posean los medios técnicos para una eventual reidentificación. Además, la legitimación de quien dese tratar estos datos deberá perfeccionarse mediante el compromiso expreso de confidencialidad y de no re-identificación, añadiendo medidas suficientes para evitar el acceso de terceros, todo ello en base al apartado 2 de la Disposición adicional decimoséptima, sobre tratamientos de datos de salud, de la Ley orgánica 3/2018.

Aunque en todo caso se tendrán en cuenta los derechos de las personas en cuanto al derecho de acceso del titular a los datos susceptibles de ser investigados, artículos 15, al derecho de rectificación, artículo 16, al derecho de limitación del tratamiento y negación de poder usar sus datos para la investigación, artículo 18, y derecho a la oposición al tratamiento de datos, artículo 21, dentro del Reglamento (EU) 2016/679.

Los derechos subjetivos de la persona para oponerse o limitar el tratamiento de sus datos no tendrá efecto cuando las investigaciones se lleven a cabo sobre datos anonimizados o seudonimizados o cuando la investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley, apartado 2.e) de la Disposición adicional 17ª de la Ley Orgánica 3/2018.

La licitud de los procesos de investigación biomédica además de cumplir con todo lo mencionado, deberán someterse al informe previo del comité de ética de la investigación y en defecto de dicho comité, se someterá al informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679, apartado 2.g) de la Disposición adicional 17ª de la Ley Orgánica 3/2018.

3.5. Tratamiento de datos personales relativos a la salud de las personas en la gestión de una epidemia-pandemia. Caso pandemia COVID-19 año 2020

3.5.1. Aspectos generales del tratamiento de datos personales relativos a la salud en la gestión de una alarma sanitaria

El capítulo 5.6 del Título I, ha tratado la cuestión del tratamiento de datos personales en la gestión de una epidemia-pandemia con una visión general sobre los datos personales.

Una vez dentro del capítulo 3 del Título III sobre el tratamiento de los datos relativos a la salud en el tratamiento de categorías especiales en Reglamento 2016/679 y Ley Orgánica 3/2018, es necesario analizar la situación que genera la gestión de una crisis sanitaria como un epidemia o pandemia sobre el tratamiento de los datos personales relativos a la salud.

Sin duda una epidemia o una pandemia es reconocida como una gravísima crisis sanitaria que afecta directamente a la salud pública y a la salud de las personas individualmente consideradas. Cuando la alerta en salud pública es debida a un proceso infectocontagioso la probabilidad de que se propague es la que justifica la propia situación de excepcionalidad de la alerta.

La AEPD publicó un informe sobre los tratamientos de datos en relación con el COVID-19 (Anexo JJ) el cual manifiesta que "el RGPD contiene reglas necesarias para permitir legítimamente tratamiento de datos personales en situaciones de emergencia sanitaria", a lo que añade que "en consecuencia, la protección de datos no debería utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades"[532].

En las aletas sanitarias producidas por una epidemia o pandemia por un proceso infectocontagioso la necesidad de contar con los datos personales de las personas afectadas justifica la aplicación de las situaciones de excepción que aparecen en el artículo 9 del Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018. En este sentido el Considerando 46 dice con relación a las epidemias:

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

3.5.2. Las excepciones al RGPD activadas a raíz de la alarma. Datos relativos a la salud

Las excepciones que devenguen de situaciones excepcionales como son las alertas en salud pública, en base al Considerando 45 del Reglamento (UE) 2016/679 deberán constar en el Derecho de la Unión o de los Estados miembros. Es decir, la excepción por sí sola no hace lícita la medida si no hay una norma suficiente que ampare las acciones que se pretenden imponer.

El artículo 9 del RGPD es el que limita y, a su vez, libera el tratamiento de los datos personales relativos a la salud, es decir, al igual que hace el artículo 6, establece límites o prohibiciones con carácter general para luego introducir puntos o cláusulas que excluyen de dichos límites o prohibiciones a determinadas situaciones o supuestos, desde un punto de vista funcional cabe entender que estas excepciones actúan como "cláusulas comodín" [533].

La prohibición del artículo 9 es clara y también lo es que esta no se aplica cuando el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, artículo 9.2.i) del Reglamento (UE) 2016/679. Así, también es el caso de la gestión de una crisis pandémica, como la del COVID-19, entrando en juego el artículo 9.2.b), por los riesgos laborales del artículo 14 y concordantes de la Ley 31/1995[534]; el artículo 9.2. g), por interés público esencial; artículo 9.2.i), por interés público en el ámbito de la salud

[532] AEPD (2020) "Informe sobre los tratamientos de datos en relación con el COVID-19". Gabinete Jurídico. Marzo 2020. Disponible en https://www.aepd.es/es/documento/2020-0017.pdf (31/05/2020).
[533] *Vid. Supra p 169,* capítulo 5.6.4.2., del Título I.
[534] Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

pública; artículo 9.2. h), por asistencia sanitario y social; y el artículo 9.2.c), por interés vital del interesado o de otra persona, por tanto, por interés vital.

Las situaciones de excepción que aparecen en el artículo 9 del Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018 contemplan como supuestos de activación, las crisis en salud pública, en consecuencia, se deben incluir las alertas sanitarias producidas por una epidemia o pandemia.

En este sentido el Considerando 46 del Reglamento (UE) 2016/679 se refiere de forma explícita a las epidemias al referir se al control de las epidemias y su propagación equiparándolas a emergencia humanitaria, catástrofes naturales o de origen humano, cuando habla que ciertos tipos de tratamiento de datos, sin especificar si son datos personales con carácter general o a datos de categorías especiales o especialmente protegidas. Así pues, el tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física o situaciones que afectan gravemente al interés público. Advirtiendo que el criterio de "interés vital de otra persona física" solo podrá apelarse cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente.

El Considerando 45 del Reglamento (UE) 2016/679 entiende que cuando exista una obligación legal relativa al responsable del tratamiento o cuando exista una actuación en interés público o cuando la acción esté ejercida por la autoridad pública, el tratamiento de los datos personales de categorías especiales debe tener una base legal en el Derecho de la Unión o de los Estados miembros.

Sin embargo, a pesar de estos Considerandos del RGPD, la Agencia Española de Protección de Datos, en su informe de abril de 2020, entiende que la base jurídica del tratamiento de datos personales durante la gestión de la pandemia por COVID-19 se establece a través de artículo 6.1e) y artículo 6.1.d) del Reglamento (UE) 2016/679 Reglamento (UE) 2016/679, sin especificar las normas del ordenamiento jurídico español que serían de aplicación o bien la necesidad de legitimar estás excepciones mediante leyes. El primero de ellos hace referencia a "la misión realizada en interés público" y el segundo "a los intereses vitales del interesado u otras personas físicas".

Por otra parte, el Considerando 52 del Reglamento (UE) 2016/679 entiende que el consentimiento del interesado podría no ser exigible para el tratamiento de categorías especiales de datos personales en casos del ámbito de la salud pública, siempre y cuando por salud pública se entienda lo definido por el Reglamento (CE) 1338/2008 del Parlamento Europeo y del Consejo, tal como dice:

> "todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad."

El mismo Considerando 52 es el que acota la excepción sobre las prohibiciones del artículo 9 del Reglamento (UE) 2016/679 por razones de interés público exclusivamente a los fines de control de la situación de alarma, pero a su vez advierte *que "no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".*

El Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, no menciona ninguna excepción al tratamiento de los datos personales relativos a la salud, por lo que los centros sanitarios, públicos y privados, han tenido que aplicar el artículo 9 en toda su extensión y solo habrán podido incluir excepciones concretas a personas concretas cuando se ha tenido que actuar en base al punto 2.i) del propio artículo 9.

3.5.3. El Estado de Alarma en la pandemia del COIVD-19 iniciada en 2020

La Ley Orgánica 4/1981, de 1 de junio de Estados de Alarma, Excepción y Sitio, en su artículo 6.1 establece que el Estado de Alarma se declara por el Consejo de Ministros mediante Real Decreto. El Estado de Alarma debe tener un carácter claramente provisional[535], hay autores que defienden su utilización en el Estado de Alarma[536], mientras hay otros autores que entienden que no debería utilizarse como un medio ordinario para la gestión de la crisis epidémica, concretamente CRUZ VILLALÓN[537].

De esta forma el Gobierno de España declara el Estado de Alarma a través del Real Decreto 463/2020[538] con motivo de que la Organización Mundial de la Salud (en adelante, también, OMS) en día 11 de marzo declara la existencia de una pandemia y dado que España en aquel momento ya tenía una cantidad importante de afectados y de muertes, concretamente, 6.023 afectados y 191 muertes, a fecha de 25/06/2020 tiene 247.086 afectados detectados y 28.327 muertes oficiales (fuente: Ministerio de Sanidad a 25/06/2020). Al Real Decreto 463/2020 le siguen otros 6 Reales Decretos de prórroga[539], y que tal como afirma ESTEVE PARDO:

[535] FERNÁNDEZ DE GATTA SÁNCHEZ, D. (2020) "El Estado de Alarma y las medidas contra el coronavirus ante jueces y tribunales", Diario La Ley, 9651. Disponible en https://diariolaley.laleynext.es/dll /2020/06/17/el-estado-de-alarma-y- las-medidas-contra-el-coronavirus- ante-jueces-y-tribunales (28/02/0221).

[536] ALEGRE ÁVILA, JM. Y SÁNCHEZ LAMELAS A. (2020) "Nota en relación a la crisis sanitaria generada por la actual emergencia vírica". Asociación española de profesores de derecho administrativo. Disponible en http://www.aepda.es/AEPDAEntrada-2741-Nota-en-relacion-a-la-crisis-sanitaria-generada- por-la-actual-emergencia-virica.aspx (28/02/2021).

[537] CRUZ VILLALÓN, P. (1984) "Estados excepcionales y suspensión de garantías". Madrid. Edi. Tecnos. p 80.

[538] Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma ocasionada por el COVID-19 (BOE núm. 67, de 14/03/2020) (estado de alarma hasta las 00:00 horas del 30 de marzo).

[539] Reales Decretos de prorroga

1. Real Decreto 476/2020, de 27 de marzo, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, (BOE núm. 86, de 28/03/2020) (1ª prórroga hasta las 00:00 horas del 12 de abril).
2. Real Decreto 487/2020, de 10 de abril, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, (BOE núm. 101, de 11/04/2020) (2ª prórroga hasta las 00:00 horas del 26 de abril).

> "De forma inédita se ha prorrogado cuatro veces sin fijarse un plazo límite claros, cuando el Estado de Alarma, por su grave y generalizada afectación a los derechos fundamentales, así como la profunda alteración al orden competencial (la nota más característica del Estado de Alarma ha sido subordinación de todas las autoridades de España a las decisiones del Gobierno) comporta una sustancial modificación de la Constitución" [540].

Posteriormente al día 11 de marzo el Gobierno de España aprueba el Real Decreto-ley 16/2020, de 28 de abril, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia y Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19.

Con objeto de comparar esta situación con las del entorno cabe decir que: Grecia aplicó las primeras restricciones el 11 de marzo cuando el país tenía 111 afectados y ninguna muerte, a fecha de 25/06/2020 tiene 3.310 afectados y 190 muertes con una población de 10.724.599 habitantes; Portugal con 78 afectados y sin ningún muerto ya había declarado el Estado de Alarma el día 12 de marzo, a fecha de 25/06/2020, tienen 40.104 afectados y 1.543 muertes con una población de 10.562.000 habitantes; Bulgaria, país miembro de la UE declaró el Estado de Excepción el día 12 de marzo de 2020 cuando tenía 23 casos confirmados y 1 muerte, a fecha de 25/06/2020 tiene 4.2422 afectados y 209 muertes, con una población de 7.000.039 habitante; por otra parte, Japón tuvo su primer caso el 23 de enero de 2020, sin utilizar Estado de Alarma, el día 25/06/2020 tiene 18.013 afectados y 967 muertes, con una población de 126.045.000 habitantes.[541]

Lay Orgánica 4/1981 dispone que el Estado de Alarma no podrá exceder de los 15 días, y que es prorrogable solo con autorización del Congreso de los Diputados. A su vez, determina que el Gobierno deberá presentar dicho Decreto a la Cámara Baja[542].

3. Real Decreto 492/2020, de 24 de abril, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. (BOE núm. 115, de 25/04/2020) (3ª prórroga hasta las 00:00 horas del día 10 de mayo).
4. Real Decreto 514/2020, de 8 de mayo, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. (BOE núm. 129, de 09/05/2020) (4ª prórroga hasta las 00:00 horas del día 24 de mayo).
5. Real Decreto 537/2020, de 22 de mayo, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. (BOE núm. 145, de 23/05/2020) (5ª prórroga hasta las 00:00 horas del día 7 de junio).
6. Real Decreto 555/2020, de 5 de junio, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 (BOE núm. 159, de 06/06/2020) (6ª prórroga hasta las 00:00 horas del día 21 de junio).

[540] ESTEVE PARDO, J. (2020) "La apelación a la ciencia …….", op.cit; pp 43 y 44.

[541] JOHNS HOPKINS UNIVERSITY (11 marzo 2020) "COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE)" at Johns Hopkins University. Disponible en https://www.arcgis.com/ apps/opsdashboard/ index.html#/bda7594740fd40299423467b48e9ecf6 (28/10/2020).

[542] Artículo 8 de La Ley Orgánica. 4/1981, de 1 de junio de Estados de Alarma, Excepción y Sitio.

El Ministerio de Sanidad con fecha 1 de octubre de 2020 publica la Resolución de 30 de septiembre, de la Secretaria de Estado de Sanidad, por la que se publica el Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud sobre la Declaración de Actuaciones Coordinadas en Salud Pública para responder ante situaciones de especial riesgo por transmisión no controlada de infecciones causadas por el SARS-Cov-2, de fecha de 30 de septiembre de 2020.

La Consejería de Sanidad de la Comunidad de Madrid presenta ante el Tribunal Superior de Justicia de Madrid la ratificación de las medidas adoptadas por la Comunidad de Madrid frente a la Orden de Ministerio de Sanidad de 30 de septiembre de 2020. El Tribunal Superior de Justicia de Madrid acuerda anular la Orden de la siguiente manera:

> "Acuerda 1. denegar, en cuanto a derechos y libertades fundamentales, la ratificación de las medidas acordadas en el apartado tercero de la Orden 1273/2020, de 1 de Octubre, de la Comunidad de Madrid, por la que establecen medidas preventivas en determinados municipios de la Comunidad de Madrid en ejecución de la Orden del Ministerio de Sanidad, de 30 de septiembre de 2020, por la que se aprueban actuaciones coordinadas en salud pública"[543].

El Gobierno del Reino de España aprobó el 2º Real Decreto de Estado de Alarma, Real Decreto 900/2020 de 9 de octubre, por el que se declara el estado de alarma para responder ante situaciones de especial riesgo por transmisión no controlada de infecciones causadas por el SARS-CoV-2. Este Real Decreto es la respuesta del Gobierno a la Sentencia del Tribunal Superior de Justicia de Madrid que con fecha de 8 de octubre de 2020 que anula la Orden del Ministerio de Sanidad.

El tercer Estado de Alamar es aprobado por el Gobierno mediante el Real Decreto 926/2020, de 25 de octubre, por el que se declara el estado de alarma para contener la propagación de infecciones causadas por el SARS-CoV-2, que viene justificado de la siguiente manera:

> "No obstante, en el momento actual en España, al igual que en la mayoría de países europeos, se registra una tendencia ascendente en el número de casos. Este incremento se ha traducido en un aumento importante de la Incidencia Acumulada en catorce días, hasta situarse, con fecha 22 de octubre, en 349 casos por 100.000 habitantes, muy por encima de los 60 casos por 100.000 habitantes que marca el umbral de alto riesgo de acuerdo a los criterios del Centro Europeo para la Prevención y Control de Enfermedades.
>
> Las actuales incidencias sitúan a todo el territorio, salvo las islas Canarias, en un nivel de riesgo alto o muy alto de acuerdo a los estándares internacionales y a los nacionales establecidos en el documento de Actuaciones de respuesta coordinada para el control de la transmisión de COVID-19, aprobado en el pleno del Consejo Interterritorial del Sistema Nacional de Salud el pasado día 22 de octubre de 2020."

Según fuentes del Ministerio de Sanidad a fecha de 25/10/2020 las cifras de prevalencia acumulada son de 1.046.132 de afectados 34.752 muertes. Cruzando estos datos con las cifras de residentes emitidas por el Instituto Nacional de Estadística (en adelante INE)

[543] ATSJM 308/2020 de 8 de octubre de 2020 (Sala de lo Contencioso) Hechos.1º (p 1) y Acuerda 1 (p 16).

que en la misma fecha era de 47.329.981 personas, se obtienen las ratios prevalencia acumulada de 22.102,9 infectados/millón de habitantes y de 734,2 fallecidos/millón de habitantes. Como referencia, el día 15/07/2020, la ratio de infectados/millón de habitantes en España era de 5.123,8 y el de muertes/millón de habitantes de 580,0 (fuentes: Ministerio de Sanidad; INE).

En base al artículo 4 del Real Decreto 926/2020 la duración del estado de alarma declarado por el presente real decreto finalizará a las 00:00 horas del día 9 de noviembre de 2020, sin perjuicio de las prórrogas que puedan establecerse.

Las limitaciones que obliga el Real Decreto 926/2020, afectan de lleno a los derechos fundamentales de la CE, y de forma explícita estas restricciones son:

1. Limitación de la libertad de circulación de las personas en horario nocturno. Del Artículo 5.
2. Limitación de la entrada y salida en las comunidades autónomas y ciudades con Estatuto de autonomía. Del artículo 6.
3. Limitación de la permanencia de grupos de personas en espacios públicos y privados. Del artículo 7.
4. Limitación a la permanencia de personas en lugares de culto. Del artículo 8.

El Real Decreto hace una remisión, a la autoridad de las Comunidades Autónomas o Ciudad Autónoma, para la puesta en marcha de las limitaciones con la siguiente expresión literal, excepto en lo que se refiera al artículo 5:

> "1. Las medidas previstas en los artículos 6, 7 y 8 serán eficaces en el territorio de cada comunidad autónoma o ciudad con Estatuto de autonomía cuando la autoridad competente delegada respectiva lo determine, a la vista de la evolución de los indicadores sanitarios, epidemiológicos, sociales, económicos y de movilidad, previa comunicación al Ministerio de Sanidad y de acuerdo con lo previsto en el artículo 13. La eficacia de la medida no podrá ser inferior a siete días naturales."

A su vez el artículo 13, "Coordinación a través del Consejo Interterritorial del Sistema Nacional de Salud.", dice:

> "Con la finalidad de garantizar la necesaria coordinación en la aplicación de las medidas contempladas en este real decreto, el Consejo Interterritorial del Sistema Nacional de Salud, bajo la presidencia del Ministro de Sanidad, podrá adoptar a estos efectos cuantos acuerdos procedan, incluidos, en su caso, el establecimiento de indicadores de referencia y criterios de valoración del riesgo. "

El Real Decreto, artículo 10, permite que las Comunidades Autónomas o Ciudad Autónoma, modulen o supriman las limitaciones de los artículos 6,7 y 8, en base al artículo 13.

El tercer estado de alarma es prorrogado mediante el Real Decreto 956/2020, de 3 de noviembre, concretamente por su artículo 1. La duración de la prorroga establecida se

extiende del día 9 noviembre de 2020 hasta el día 9 de mayo de 2021, ambos a las 00:00h[544].

3.5.4. El estudio de la movilidad de las personas aplicada a la crisis sanitaria

En España se autorizó a través de la Orden SND/297/2020, de 27 de marzo, la encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, del desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19, en base al Real Decreto 463/2020. Lo cual ha llevado al estudio de la movilidad aplicada a la crisis sanitaria, de forma agregada y anonimizada.

La pregunta que surge no puede ser otra que ¿es suficiente una Orden Ministerial para la autorización de un estudio de tipo? ¿Qué control se ha establecido en cuanto al alcance y utilización de los datos necesarios para llevar a cabo tal estudio?

En otros países del mundo, que a de la Orden mencionada, China y Corea del Sur estaban utilizando una aplicación para smartphones desarrollada por el Ministerio del Interior y Seguridad de China, conocida como "self-quarantine safety protection"[545]. Esta aplicación permite varias funciones, entre las cuales está la de monitorizar el movimiento de los ciudadanos mientras estén en cuarentena, lo cual avisa al centro de control cuando un ciudadano sale de la zona autorizada.

El supuesto que plantea la aplicación utilizada en Corea del Sur y China tan solo podría ser aplicado en la Unión Europea, y por tanto en España, en virtud de una norma de rango suficiente que lo autorizara en base al punto 2.i) del artículo 9 del Reglamento (UE).

Es muy discutible que esa norma con rango suficiente pueda ser tan solo una norma con rango reglamentario nacional cuando se trata de una norma que va a regular derechos fundamentales, como es la protección de datos de carácter personal, sobre el que la Constitución Española, artículo 53 CE establece una reserva de ley[546].

En los casos de materias reservadas a la Ley, como es este caso, cabe la colaboración reglamentaria, pero siempre que la ley haya establecido previamente los aspectos nucleares o esenciales de la regulación y siempre que esa regulación reglamentaria sea "claramente dependiente y subordinada a la ley" tal y como viene reiterando de forma asentada y univoca desde la aprobación de la Constitución Española el Tribunal Constitucional[547].

[544] Artículo 2 del Real Decreto 956/2020, de 3 de noviembre, por el que se prorroga el estado de alarma declarado por el Real Decreto 926/2020, de 25 de octubre, por el que se declara el estado de alarma para contener la propagación de infecciones causadas por el SARS-Cov-2.

[545] OECD. Tracking and tracing COVID: protecting privacy and data while using APPS and Biometrics. OECD 2020. Updated 23 April 2020. Disponible en https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/ (31/01/2021).

[546] *Vid. Supra p 79,* capítulo 2.3.1.1.1., del Título I.

[547] STC 83/1984, y reiterada en otras recientes, así STC 111/2014 y STC 139/2016.

3.5.5. El supuesto de la toma de la temperatura corporal dentro del RGPD

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

La AEPD entiende que esta acción, la toma de temperatura en espacios públicos, tendría efectos sobre ciertos derechos inalienables. Esta toma de datos relativos a la salud de las personas además de devenir en eventuales denegaciones de acceso en centro laboral, educativo o comercial, desvelaría a terceros la temperatura corporal de la persona interesada y a su vez desvelaría que este dato de salud estaría por encima del estándar establecido y que, en consecuencia, dada la situación general, es subsidiaria de estar padecimiento la enfermedad del COVID-19, lo cual contraviene el RGPD. No cumpliría el principio de confidencialidad, artículo 5.5 y artículo 36.1.c) del Reglamento (UE) 2016/679.

Cualquier acción en este sentido requeriría una regulación legislativa que pusiera límites y garantías, plazos de conservación y de destrucción de los datos, para el tratamiento de los datos personales relativos a la salud de las personas afectadas, tal como consta en el artículo 9, letras g), h) e i) del Reglamento (UE) 2016/679[548].

La toma de temperatura puede realizarse de forma manual o a través de medios tecnológicos. Las cámaras de video sensibles a los rayos infrarrojos cámaras terminas, son uno de estos elementos tecnológicos cuyos datos están bajo el manto normativo del RGPD. En el caso de que la técnica de toma del dato fuera la de la cámara, activa otro principio del RGPD, el principio de limitación de la finalidad, artículo 5.1.b) del Reglamento (UE) 2016/679. Este principio hace constar que:

> "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales."

Como conclusión de este punto, bajo ningún concepto, estos datos obtenidos mediante cámaras podrían ser usados para otro fin o lo que es peor, no podría usarse el dispositivo, cámaras térmicas, para captar o tratar otros datos distintos a la temperatura corporal de la persona.

[548] AEMM (8 mayo 2020) Asociación de Empresas del Metal de Madrid. Comunicado "Consideraciones sobre los controles de temperatura corporal y protección de datos en el marco de la crisis del COVID-19". Disponible en https://www.aecim.org/consideraciones-sobre-los-controles-de-temperatura-corporal-y-proteccion-de-datos-en-el-marco-de-la-crisis-del-covid-19/# (31/05/2020).

Otro principio del Reglamento (UE) 2016/679, el principio de exactitud de los datos, artículo 5.1.d) obligaría que la base jurídica que debería abordar el Gobierno a través del Ministerio de Sanidad incluyera las condiciones de calibración y recalibración de los medidores.

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

Por otra parte, en cuanto al escenario laboral, podría actuar como excepción. El acto de toma de temperatura corporal encajaría dentro de lo dispuesto en el artículo 9.2.b). en base a las obligaciones que tiene el empleador en cuanto a la seguridad y protección de la salud del trabajador[549], lo cual no impide que se cumpla la legitimación exigida en el artículo 9.2.h) del Reglamento (UE) 2016/679 así como el resto de los principios que protege el RGPD.

Así pues, en este orden de cosas, exceptuando la licitud del tratamiento de datos específicamente eximido de la prohibición del artículo 9.1 y cumpliendo las exigencias de legitimidad de la persona que los vaya a tratar, este tratamiento de datos, eximido de prohibición, deberá realizarse respetando tanto los principios y derechos aplicables a cualquier tipo de datos personales como aquellos principios y derechos que adquieren los datos relativos a la salud o a otras categorías de datos protegidas, tal es el caso de mantener el máximo nivel de confidencialidad, protección de la intimidad, protección de la privacidad, protección del honor, principio de la protección de la autonomía de la voluntad como expresión del principio de la libertad de la persona en todo lo que afecte a la excepción legitimadora. Además, se deberán respetar los principios de limitación de la finalidad, minimización de los datos, exactitud, confidencialidad, limitación del periodo de conservación de los datos, calidad de los datos, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes.

A su vez, la persona seguirá estando en posesión de sus derechos tales como el derecho de acceso, de rectificación, el de supresión cuando no haya una oposición médica, derecho a la limitación justificada que no obstaculice la causa que eximió la prohibición del artículo 9.1, el derecho a la portabilidad y el derecho a la oposición, salvo que el responsable del tratamiento aluda a motivos legales, legítimos o imperiosos.

Para concluir, la persona mantendrá todos los derechos que le amparan en cuanto al derecho a presentar una reclamación ante una autoridad de control, al derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento, el derecho a representación del interesado y al derecho a indemnización y responsabilidad, artículos 77 al 82 del Reglamento (UE) 2016/679.

[549]Artículo 15 de la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales.

3.5.6. El supuesto de la realización de test del COVID-19 como detector de infectados para acceder al puesto de trabajo dentro del RGDP

El diagnóstico de la infección del virus SARS-CoV-2, conocido como COVID-19, se realiza por un conjunto de síntomas, signos y circunstancias, no tan solo mediante una sola prueba de laboratorio, tal como afirma el Hospital Clínic de Barcelona en su web[550]:

> "El diagnóstico de cualquier enfermedad depende de la historia y del conjunto de síntomas y signos que presente el paciente, valorando la situación epidemiológica y otros muchos datos interpretados por el profesional. No hay una sola prueba diagnóstica, sino que incluye varias posibilidades. A partir de aquí, se considera y valora la práctica de determinadas exploraciones complementarias y pruebas de laboratorio."

Las pruebas diagnósticas de laboratorio más conocidas para la detección de la infección del virus SARS-CoV-2 son tres[551]:

- Pruebas de detección de ácidos nucleicos (reacción en cadena de la polimerasa o PCR)
- Pruebas de detección de antígeno
- Pruebas de detección de anticuerpos (IgG, IgM)

Las pruebas de detección de ácidos nucleicos también conocidas por PCR, es una técnica de biología molecular de detección de material genético, ARN, del SARS-CoV-2 en distintas muestras biológicas clínicas. Según todos los expertos es la principal prueba de laboratorio para el diagnóstico de COVID-19[552] (Anexo[KK]). Las muestras suelen ser de mucosa nasofaringe, aunque también podría utilizarse orina, heces e incluso sangre. El tiempo de la prueba es de unas 4 horas. La sensibilidad es entorno al 95% y una especificidad del 100%[553]. Es precoz porque se detecta virus en las primeras fases de la infección[554]. Se están introduciendo variantes para la PCR-rápida, de 45 minutos.

> "La sensibilidad de la prueba diagnóstica se define como la probabilidad de que el resultado de la prueba sea positivo (h+) en una persona afectada por la enfermedad (e+). La especificidad de la prueba diagnóstica se define como la probabilidad de que el

[550] PORTAL CLINIC (12 marzo 2020) "Diagnóstico del Coronavirus SARS-CoV-2". Hospital Clinic de Barcelona. Disponible en https://www.clinicbarcelona.org/asistencia/enfermedades/covid-19/diagnostico (31/01/2021).

[551] AEPap. (12 abril 2020) "Pruebas diagnósticas de laboratorios de COIVD-19". Asociación Española de Pediatría de Atención primaria. Disponible en https://www.aepap.org/sites/default/files /documento/ archivos-adjuntos/pruebas_diagnosticas_de_laboratorio_de_covid_vfinal.pdf (31/05/2020).

[552] CONSEJERÍA DE SANIDAD. MADRID (2020) "Procedimiento de detección del nuevo coronavirus SARS-CoV-2 en la Comunidad de Madrid". Dirección General de Salud Pública. Red de Vigilancia Epidemiológica. Disponible en https://www.comunidad.madrid/sites/default/ files/doc/sanidad/epid / procedimiento_de_deteccion_del_nuevo_coronavirus_sars-cov-2_en_cm.pdf (31/05/2020).

[553] CORMAN V. M. ET AL. (2020) "Detection of 2019 novel coronavirus (2019-nCoV) by real-time RT-PCR". Eurosurveillance: Revista europea sobre vigilancia de enfermedades infecciosas, epidemiología, prevención y control, 25 (3), 23-30. Disponible en doi: 10.2807 / 1560-7917.ES.2020.25.3.2000045 (28/02/2021).

[554] GONZÁLEZ FEIJOO M. (2020) "Todo lo que debes saber sobre los tests de diagnóstico de COVID-19". EnfermeríaTV. Disponible en https://enfermeriatv.es/es/el-mejor-metodo-diagnostico/ (31/01/2021).

> resultado de la prueba sea negativo (h-) en una persona sana, que no padece la enfermedad (e-). Por tanto, representa la fracción de verdaderos negativos[555].

La prueba de detección de antígenos, se basan en la detección de proteínas virales específicas de SARS-CoV-2 en la muestra tomada del paciente, tales como la proteína N y las subunidades S1 o S2 de la proteína espiga. Estas proteínas forman parte de una especie de cápsula que envuelve al ARN viral o genoma viral[556]. Se utiliza la misma muestra que en el caso de los PCR. Este tipo de pruebas a día hoy aun presentan incógnitas tales como su baja sensibilidad[557]. Hasta la fecha, son poco aconsejables[558].

La prueba de detección de anticuerpos se hace sobre una muestra de sangre de origen capilar, suero o plasma buscando la presencia de anticuerpos IgM e IgG frente SARS-CoV-2. Tras la infección se genera IgM entre los 5-7 días tras la infección, los test los detectan entre los 8-14 días. Los anticuerpos IgG aparecen trascurridos entre 15-21 días de la detección de virus por el sistema inmunológico[559]. Los resultados de la prueba se obtienen en 15 minutos. Un resultado positivo indicaría infección por SARS-CoV-2, aunque existe la posibilidad de falsos positivos por reacción cruzada con otros coronavirus humanos y otros virus[560], pero también se han encontrado falsos negativos[561]. Lo cual obliga a tomar medidas confirmatorias cuando hay cualquier tipo de duda.

La medida de utilizar los test de diagnóstico para detectar infectados antes de que se incorporen a sus puestos de trabajo y en consecuencia permitir su incorporación ha sido ampliamente comentada por la prensa. La empresa SEAT justificaba el día 22 de abril de 2020 con un comunicado, la adopción de la medida diciendo:

> "La vuelta al trabajo será paulatina y solo para los trabajadores que no estén dentro de los grupos de riesgo, que se irán reincorporando más adelante. La compañía ha diseñado

[555] SEGURA EGEA JJ. (2002) "Sensibilidad y especificidad de los métodos diagnósticos convencionales de la caries oclusal según la evidencia científica disponible". RCOE (revista del Ilustre Consejo General de Colegios de Odontólogos y Estomatólogos de España), 7 (5), 491-501. Disponible en http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1138-123X2002000600004 (31/05/2020).

[556] AEPap. (12 abril 2020) "Pruebas diagnósticas de laboratorios de COIVD-19". Asociación Española de Pediatría de Atención primaria. Disponible en https://www.aepap.org/sites/default/files/ documento/ archivos-adjuntos/pruebas_diagnosticas_de_laboratorio_de_covid_vfinal.pdf (31/05/2020).

[557] OMS. (8 April 2020) "Advice on the use of point-of-care immunodiagnostic tests for COVID-19". World Health Organization. Scientific brief. Disponible en https://www.who.int/docs/default-source/ coronaviruse/ sb-2020-1-poc-immunodiagnostics-2020-04-08-e.pdf? sfvrsn=4c26ac39_2 (31/01/2021).

[558] BBC News (25 abril 2020) "Tests de coronavirus: cómo son las pruebas serológicas y moleculares para detectar el covid-19 y qué ventajas e inconvenientes". Disponible en https://www.bbc.com/mundo /noticias-52361548 (31/05/2020).

[559] SEI (2 de abril de 2020) "Utilidad de la determinación de anticuerpos anti SARS-CoV-2. Propuesta de implementación como prueba diagnóstica, pronóstica y de desarrollo de inmunidad protectora". Sociedad Española de Inmunología. Version 01. Disponible en https://www.micof.es/bd/ archivos/ archivo15001.pdf (31/01/2021).

[560] LOEFFELHOLZ MJ. TANG, YI-WEI (2020) "Laboratory diagnosis of emerging human coronavirus infections – the state of the art". Emerging Microbes & Infections. 9 (1), 747-756. Disponible en https://doi.org/10.1080/22221751.2020.1745095 (28/02/2021).

[561] THEIMER S. (2020) "Falsos negativos en prueba de COVID-19 pueden llevar a errónea sensación de seguridad". Mayo Clinic News Network. Disponible en https://newsnetwork.mayoclinic.org/discussion/ falsos-negativos-en-prueba-de-covid-19-pueden-llevar-a-erronea-sensacion-de-seguridad/ (31/01/2021).

> un protocolo sanitario específico para garantizar la distancia de seguridad de dos metros, la dotación de máscaras quirúrgicas, geles desinfectantes y la limpieza de las instalaciones antes y después de cada turno de trabajo."

La base legal de esta acción habrá que buscarla en el artículo 9 del Reglamento (UE) 2016/679, concretamente en su apartado 2 letra b) que dice:

> "b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;"

A lo cual hay que añadir que el artículo 22 -Vigilancia de la Salud- de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales, dice en punto 1. "El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo".

En cuanto a la confidencialidad exigida por el RGPD también lo es por la Ley 31/1995, en su artículo 22.2 exige que toda esta medida se lleve a cabo "respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud."

En cuanto a la obligación del consentimiento del sujeto interesado, esta obligación es eximida por el artículo 9.2.b) del Reglamento (UE) 2016/679, lo cual ya venía exonerado en el artículo 22.1 de la Ley 31/1995, pues:

> "1. (…) este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad."

Las dos centrales sindicales mayoritarias en España, UGT y CCOO, manifestaron que no tan solo no se oponían a la realización del test antes de incorporarse al puesto de trabajo, sino que incluso, lo exigína. Así Europapress[562] publicaba el 16/04/2020 "UGT exige test de detección de Covid-19 para el personal de supermercados". Por su parte CCOO publicaba en su web[563] el día 08/05/2020 "CCOO exige la realización del test de COVID-19 de máxima fiabilidad al personal que trabaja en el sector de la dependencia".

[562] FERNÁNDEZ JARA, M, (16 abril 2020) "UGT exige test de detección de Covid-19 para el personal de supermercados". Europa Express. Disponible en https://www.europapress.es/cantabria/noticia-ugt-exige-test-deteccion-covid-19-personal- supermercados-20200416135425.html (30/04/2021).

[563] CCOO (8 mayo 2020) "CCOO exige la realización del test de Covid 19 de máxima fiabilidad al personal que trabaja en el sector de la dependencia". Comisiones Obreras de Andalucía 8 mayo 2020. Disponible en https://andalucia.ccoo.es/noticia:493424--CCOO_exige_la_realizacion_del_test_de_Covid_19_de_ máxima

En este orden de cosas, parece que la obligatoriedad de la realización de la prueba del COVID-19 para conocer si la persona padece la enfermedad y en consecuencia no permitir que se incorpore al centro de trabajo hasta dar por curada dicha enfermedad, está fundamentada en derecho y respeta el principio de legalidad, lo que no es excusa para no hacer notar que, aun así, puede afectar gravemente a los derechos de las personas.

3.5.7. El Supuesto del "pasaporte o carne de inmunidad" del COVID-19 dentro del RGPD

Este punto se desarrolla en base al desarrollo de la inmunología a fecha de mayo-diciembre de año 2021. Desde el inicio de la pandemia ha habido un cambio de posturas de las autoridades tanto nacionales como de la Unión Europea.

Muchos de medios comunicación publicaron durante la primera mitad de crisis pandémica de 2020 noticias relativas a lo que se ha venido a llamar "carné de inmunidad del COVID-19". Como ejemplo de esta difusión con relación a esta idea, se trae una muestra como puede ser que, con fecha de 22 de abril de 2020, BBC News publica un artículo con una definición sobre el carné de inmunidad del COVID-19 (BBC News, abril 2020)[564]: "comprobar que alguien ha pasado el SARS-Cov-2 y es inmune al virus, y otorgarle un carné, pasaporte o certificado que lo constate."

Con fecha de 7 de abril de 2020, Redacción médica[565] publicaba: "Coronavirus España: nace el primer carné de inmunidad al Covid-19". Sin embargo, el día 8 de abril de 2020, el Ministro de Sanidad declara que "descarta que se vaya a crear un carné de inmunidad del Covid-19 como ha hecho Castilla y León"[566].

Otros rotativos mostraban serias discrepancias con esta idea, tal es el caso de El País de 14 de abril de 2020 [567] que titulaba: "Un carné de inmunidad es una estupidez enorme".

Con fecha de 14 de abril de 2020, el periódico Crónica Global[568] titulaba la noticia como: "Torra y Mitjà proponen clasificar a los ciudadanos y seguirles por el móvil" para después explicar que: "El informe del epidemiólogo (se refiere al informe del Mitja), que aún no es

_fiabilidad_al_personal_que_trabaja_en_el_sector_de_la_dependencia&opc_id=434bdbdecfdacb8f5f4e92b187bd73a0 (31/01/2021).

[564] GIL, T (22 abril 2020). "Medidas contra el coronavirus: qué es el "pasaporte o carné de inmunidad" a la covid-19 y por qué genera polémica". BBC News. Disponible en https://www.bbc.com/mundo/ noticias-52377212 (31/05/2020).

[565] MEDIAVILLA, J. (7 abril 2020) "Coronavirus España: nace el primer carnet de inmunidad al Covid-19". Redacción médica. Disponible en https://www.redaccionmedica.com/autonomias/ castilla-leon/coronavirus-espana-nace-el-primer-carnet-de-inmunidad- al-covid-19-4009 (31/05/2020).

[566] INFOSALUS (1 abril 2020) "Illa descarta que se vaya a crear un carnet de inmunidad del Covid-19 como ha hecho Castilla y León. Disponible en https://www.infosalus.com/salud-investigacion/noticia-illa-descarta-vaya-crear-carnet-inmunidad-covid-19-hecho-castilla-leon-20200408203016.html (31/01/2021).

[567] VERDÚ D. (14 abril 2020) "Un carné de inmunidad es una estupidez enorme". El País. Disponible en https://elpais.com/sociedad/ 2020-04-14/ un-carne-de-inmunidad-es-una-estupidez-enorme.html (31/05/2020).

[568] JORRO, I. (19 abril 2020) "Torra y Mitjà proponen clasificar a los ciudadanos y seguirles por el móvil". Crónica global. Disponible en https://cronicaglobal.elespanol.com/politica/torra-oriol-mitja-codigo-colores_339648_102.html (31/01/2021).

público, apuesta por salir de la pandemia con un "pasaporte de inmunidad" para acceder a grandes eventos; un certificado digital que indique el estado de salud de la persona".

Concretando, la idea de un pasaporte de inmunidad del COIVD-19 como aquel "carné que certifica que una persona es inmune al COVID-19", como consecuencia de haber estado en contacto con el virus, surgió en el año 2020 gozando de poco predicamento científico.

La OMS en el año 2020 no apoyaba la iniciativa, en este orden de cosas, El País el día 25 de abril de 2020[569], titula: "La OMS rechaza el pasaporte inmunitario por falta de evidencia sobre el riesgo de segundas infecciones". Este tipo de certificados, que identifican quién ha pasado la enfermedad, podría "aumentar los riesgos de transmisión". El día 25 de abril de 2020, La vanguardia [570] tituló: "OMS: El "pasaporte de inmunidad" contra el Covid no tiene respaldo científico".

El único método predictor de esta inmunidad es el estudio inmunológico de la persona a estudiar, a través de la detección de IgM e IgG en su sangre. Distintos expertos criticaron la utilización de esta técnica para expedir carnés de inmunidad al igual que han criticado los propios carnets de inmunidad. El Dr. Ildefonso Hernández, exdirector general de Salud Pública de España (2008-2011) y actual portavoz de la Sociedad Española de Salud Pública declaró en la BBC News de 22 de abril de 2020 "Desde el punto de vista de la factibilidad, hoy por hoy es una imprudencia utilizar esto", añadiendo "las pruebas rápidas de anticuerpos, que son las propuestas para determinar la inmunidad, tienen una exactitud limitada"[571].

Las dudas sobre la inmunidad permanente de las personas afectadas frente al COVID-19 es evidente. El Dr. Fernando Fariñas en el 21 de marzo de 2020 en la publicación de la Fundación IO[572] manifiesta "En la defensa frente a todos los coronavirus, se ha demostrado que no solo es importante la producción de anticuerpos neutralizantes, sino también de inmunidad celular de tipo Th1 con activación de células CD8 + citotóxicas y NK."

[569] MAUZO, J. (25 abril 2020) "La OMS rechaza el pasaporte inmunitario por falta de evidencia sobre el riesgo de segundas infecciones". El País. Disponible en https://elpais.com/sociedad/2020-04-25/la-oms-rechaza-el- pasaporte-inmunitario-por-falta-de-evidencia-sobre-el-riesgo-de-segundas- infecciones.html (28/02/2021).

[570] LA VANGUARDIA (25 abril 2020) "OMS: El "pasaporte de inmunidad" contra el Covid no tiene respaldo científico". Disponible en https://www.lavanguardia.com/vida/20200425/48714129316/oms-pasaporte-inmunidad-covid.html (31/01/2021).

[571] GIL, T (22 abril 2020). "Medidas contra el coronavirus: qué es el "pasaporte o carné de inmunidad" a la covid-19 y por qué genera polémica". BBC News. Disponible en https://www.bbc.com/mundo/ noticias-52377212 (31/05/2020).

[572] FUNDACIÓN IO (21 marzo 2020) "¿Inmunología Clínica del COVID-19 Qué sabemos hasta ahora?". Disponible en https://fundacionio.com/2020/03/21/inmunologia-clinica-del-covid19-que-sabemos-hasta-ahora-por-el-dr-fernando-farinas/ (31/01/2021).

El artículo científico[573], seleccionado por el Servicio Gallego de Salud[574], entiende que las decisiones políticas deben esta sustentadas en ciencia y que hasta el momento solo hay conjeturas sin evidencia ciencia contrastada. Este artículo dice: "Science must also guide policy decisions. Reliance on comprehensive seroprevalence data and a solid, research based grasp of correlates of protection will allow policy to be guided by secure, evidence-based assumptions on herd immunity, rather than optimistic guesses".

El estudio de esta acción no encontró en el año 2020 base legal para que se puede llevar a cabo en base al conocimiento que tiene la ciencia de la inmunidad de las personas y en base a los principios que exige el Reglamento (UE) 2016/679.

El principio de limitación de la finalidad, artículo 5.1.b) del Reglamento (UE) 2016/679 y expuesto en el Considerando 39 expresan que todo tratamiento de datos personales debe ser lícito y leal, en el sentido de que los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. En este orden de cosas, la duda sobre la utilidad de la detección de anticuerpos, hoy en día, manifiesta que el carné de inmunidad frente al COVID-19 no tiene en cuenta el principio de limitación de finalidad del RGPD.

Por otra parte, es evidente que la detección de unos anticuerpos y la expresión de este dato en un carné que califique al que lo tiene como ha sufrido una determinada infección y la posibilidad de que este carné sea visto por terceras personas, sin garantías posibles y razonables de limitar dicho acceso, hace poner en peligro el principio de confidencialidad del artículo 5.1.f) del Reglamento (UE) 2016/679. Es el Considerando 39 el que recuerda que la confidencialidad también implica impedir el acceso o uso no autorizado a los datos protegidos.

En cuanto al soporte legal de su legitimación, no hay ningún supuesto del artículo 6 del Reglamento (UE) 2016/679 que exonere de la necesidad del consentimiento de la persona. Sin embargo, si el RGPD exige que el consentimiento debe ser absolutamente libre, cabe preguntarse si esta exigencia se cumple.

En este orden de cosas, si la Administración pública obligara a que el ciudadano estuviera en disposición de un carné que certificara su inmunidad frente al COVID-19 para poder ejercer el derecho a la libre circulación y movilidad entre la limitación a otros derechos, cabe preguntarse si es razonable suponer que un ciudadano puede llevar una vida social y laboral normal sin ese carné. Siguiendo con la argumentación, y si es así, cabe preguntarse si es razonable creer que un ciudadano vaya a negar dar su consentimiento a dicho carné. Con todo ello, el consentimiento no sería libre sino totalmente impuesto.

La limitación de la movilidad es inconstitucional dado que el artículo 19 de la Constitución Española de 1978 expresa un derecho fundamental que determina que los españoles tienen

[573] ALTMANN DM, ET AL. (2020) "What policy makers need to know about COVID-19 protective immunity". Lancet, 395. https://doi.org/10.1016/S0140-6736(20)30985-5. (28/02/2021).

[574] SERGAS (2020). "Estudios seleccionados sobre SARS-CoV-2 y COVID-19". Consejería de Saude. Disponible en https://coronavirus.sergas.gal/Contidos/Documents/216/ Seguimiento_Publicacions_ COVID19_ 08052020.pdf (31/01/2021).

derecho a elegir libremente su residencia y a circular por el territorio nacional, el cual en base a lo expuesto en el Capítulo 2.3.1 del Título I, la limitación de un derecho fundamental requiere de una Ley Orgánica y del respeto al contenido esencial del derecho fundamental y al criterio de ponderación.

Por otra parte, si el cané de inmunidad hubiera que presentarlo en lugar público y sin protección de la intimidad, se vulneraría el derecho fundamental de confidencialidad expresado en el Artículo 18 de la Constitución Española. Además, también el deber de confidencialidad expresado en los artículos 5 y 32 del Reglamento (UE) 2016/679.

La medida del carné de o pasaporte de inmunidad y su aplicación haría entrar en conflicto varios derechos constitucionales lo cual requeriría una norma con rango de Ley orgánica para su regulación. En el caso de España, se deben tener presentes tanto las reservas de Ley indicadas por la Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales como la reserva de Ley orgánica del artículo 81 de la Constitución Española, al regular cuestiones relativas a los derechos fundamentales.

En conclusión, el informe 0017/2020 de la AEPD manifiesta que las consideraciones relacionadas con la protección de datos -dentro de los límites previstos por las leyes- 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, pero no está de más recordar a AEPD que no es menos cierto que el RGPD es muy claro y es solo este el que determina los tipos de exclusiones posibles y, sobre todo, en las condiciones en las que se puede dar, lo cual obliga a los Estados Miembros a no relajar la protección de los derechos fundamentales y cumplir con las reservas de ley exigidas.

Es evidente que una medida de esta naturaleza precisaría de un Reglamento del Parlamento Europeo y de la Comisión de la UE que sentara las bases legales para su puesta en marcha y sentara las bases legales para sus fines y exigibilidad.

El capítulo 3.2. del Título IV, en la página 442, expone las declaraciones de la Comisión Europea en relación a esta cuestión y el Reglamento sobre el Certificado Digital Verde que la Comisión y el Parlamento están preparando durante el primer semestre de 2021, que luego acabo por llamarse Certificado Digital UE-COVID. De tal forma el 20 de mayo de 2021 la web de la Comisión Europea publica: “Certificado COVID Digital de la UE: el Parlamento Europeo y el Consejo alcanzan un acuerdo sobre la propuesta de la Comisión.”

Capítulo 4. La Autoridad de control dentro de la protección de datos del sector de la salud

4.1. La figura de las autoridades de control dentro de la protección de datos del sector de la salud

La Autoridad de control para el RGPD es la autoridad pública independiente establecida por un Estado miembro con arreglo al artículo 51 del Reglamento (UE) 2016/679, definida en el artículo 4.21 del Reglamento (UE) 2016/679.

Para supervisar la aplicación del RGPD cada Estado miembro de la UE creará o designará una o varias Autoridades de Control adecuadamente dotadas, aunque si hay varias, una será la principal. Esta supervisión independiente de cualquier institución tendrá dos objetivos, el material, en cuanto al cumplimiento formal coherente de la normativa excepto en la acción de los tribunales en su función jurisdiccional, artículo 55.3 del Reglamento (UE) 2016/679, y el subjetivo, en cuanto a la protección efectiva de los derechos y libertades de libre circulación de las personas dentro de la Unión Europea, artículo 51 y 52 del Reglamento (UE) 2016/679.

Independientemente de la competencia de resolver reclamaciones en materia de protección de datos, la Autoridad de control debe controlar la aplicación del Reglamento (UE) 2016/679 y hacerlo aplicar, artículo 57.1.a) del Reglamento (UE) 2016/679, además dispone del poder de sancionar, artículo 58.2 del Reglamento (UE) 2016/679.

El artículo 9 del Reglamento (UE) 2016/679 que prohíbe el tratamiento de los datos relativos a la salud, establece en su apartado 2 una serie de excepciones y en el apartado 3, bases jurídicas para su ejercicio. La Autoridad de control tiene, entre sus diversas funciones, las de asesorar a las instituciones[575], también a las sanitarias públicas y privadas, sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.

Sin duda las organizaciones en las cuales se utilicen datos de salud de las personas necesitarán realizar un adecuado análisis del impacto y la Autoridad de control deberá disponer de una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, artículo 57.1.h) del Reglamento (UE) 2016/679.

La Autoridad de control, en el ámbito sanitario, podrá llevar a cabo investigaciones en forma de auditorías de protección de datos, obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones y obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos.

[575] AEPD (2019) "La protección de datos y la Administración Local" Guías sectoriales AEPD. Septiembre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf (31/01/2021).

La Autoridad de control dispone de la potestad para asesorar al responsable del tratamiento conforme al procedimiento de consulta previa[576] contemplado en el artículo 36 del Reglamento (UE) 2016/679, artículo 58.3 del Reglamento (UE) 2016/679.

4.2. Relación en casos especiales

En el capítulo 2 del Título II se ha tratado la figura de la Autoridad de control tal como la crea, define y regula el Reglamento (UE) 2916/679. En este apartado 2 del capítulo 4 del Título III, se pretende ver la relación de la Autoridad de control con las situaciones especiales que pueda conllevar el dato personal relativo a la salud o con los responsables de los tratamientos de datos a lo que se refiere el artículo 9 del Reglamento (UE) 2016/679.

Lo datos de salud son datos cuyo tratamiento está especialmente protegido y que en consecuencia se deberá garantizar la seguridad de este, artículo 32 del Reglamento (UE) 2016/679, iniciando precauciones ya desde el diseño, artículo 25 del Reglamento (UE) 2016/679, y en especial analizando los riesgos para los derechos enunciados por el RGPD mediante evaluación del impacto relativa a la protección de datos, artículo 35.1 del Reglamento (UE) 2016/679.

La primera relación que el Reglamento (UE) establece entre la Autoridad de control y el dato relativo a la salud, es precisamente en la evaluación del impacto[577] relativas a la protección de estos datos[578]. Concretamente el artículo 35.4. del Reglamento (UE) 2016/679 ordena a la Autoridad de control la realización y su publicación de listas de los tipos de operaciones de tratamiento que requieran una evaluación de impacto en el escenario de los datos de salud.

La segunda relación que el Reglamento (UE) establece entre la Autoridad de control y el dato relativo a la salud, se manifiesta en el supuesto relativo a la consulta previa realizada por un responsable del tratamiento de datos. El responsable del tratamiento de datos relativos a la salud frente a cualquier duda o exceso de riesgo sobre la autorizado por el RGPD realizará una consulta previa a la Autoridad de control, artículo 36.1 del Reglamento (UE) 2016/679 [579]. Si con motivo de la consulta la Autoridad de control considera que el tratamiento de datos confiere elevados riesgos en base a RGPD, en un plazo de ocho semanas, prorrogable seis semanas, desde la solicitud de la consulta, la Autoridad de control deberá remitir por escrito al responsable o al encargado de la forma correcta de actuar, pudiendo utilizar si fuera preciso cualquier potestad conferida en el artículo 58 del Reglamento (UE) 2016/769, tales son, entre otras, las de investigar, ordenar, limitar, prohibir y sancionar.

[576] *Vid. Supra p 222,* capítulo 3.7., del Título II.

[577] *Vid. Supra p 210,* capítulo 3.6., del Título II.

[578] AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (31/01/2021).

[579] AEPD (2021) "Formulario de Consulta Previa". Disponible en https://sedeagpd.gob.es/sede-electronica-web /vistas/formConsultaPrevia/procedimientoConsultasPrevias.jsf. (31/01/2021)

La tercera relación que el Reglamento (UE) establece entre la Autoridad de control y el dato relativo a la salud, viene a través de la garantía que deberá dar el Gobierno, en todo caso, de que la Autoridad de control sea consultada[580] durante la elaboración de toda propuesta de medida legislativa o de una medida reglamentaria que se refiera al tratamiento, artículo 36.4 del Reglamento (UE) 2016/679, y según se desprende del RGPD, en especial en los supuestos del artículo 9.

[580] AEPD (2019) "Funciones y poderes". Enero de 2019. Disponible en https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/funcion-y-poderes (28/02/2021).

Capítulo 5. El responsable y el encargado del tratamiento de datos en el sector de la salud

5.1. El responsable del tratamiento de datos en el sector de la salud

En base al artículo 4.7) del Reglamento (UE) 2016/679 el responsable del tratamiento o responsable "es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento".

El Reglamento (UE) 2016/679 también hace referencia al corresponsable del tratamiento. En este sentido, cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Estos deberán acordar sus responsabilidades respectivas en especial en lo referente al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información, artículo 26 del Reglamento (UE) 2016/679.

El Considerando 22 del Reglamento (UE) 2016/679 entiende que todo tratamiento de datos personales en el contexto de las actividades de un establecimiento implica a un responsable. En consecuencia, el responsable del tratamiento corresponde a la persona responsable del establecimiento que utiliza los datos protegidos por el RGPD.

El responsable del tratamiento será responsable del cumplimiento de los principios relativos al tratamiento, dispuesto en el apartado 1 del artículo 5 del Reglamento (UE) 2016/679, y deberá ser capaz de demostrarlo, en base al principio de responsabilidad proactiva, Considerando 85 del Reglamento (UE) 2016/679.

El responsable del tratamiento a fin de garantizar y poder demostrar que el tratamiento es conforme con al Reglamento (UE) 2016/679, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas aplicará medidas técnicas y organizativas apropiadas, artículo 24.1 del Reglamento (UE) 2016/679, a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad garantizando que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas, artículo 25.2 del Reglamento (UE) 2016/679.

En este orden de cosas, al estar los datos relativos a la salud especialmente protegidos por el artículo 9 del Reglamento (UE) 2016/679, el responsable aplicará las máximas garantías de protección en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización y la minimización de datos, e integrar las garantías necesarias en el tratamiento, artículo 25.1 del Reglamento (UE) 2016/679.

En cuanto a los datos relativos a la salud de las personas, el responsable del tratamiento de los datos es el responsable del establecimiento asistencial o no asistencial que utiliza los datos protegidos por el RGPD relativos a la salud de las personas, a su vez, protegidos especialmente por el artículo 9 del reglamento. Con relación a los datos relativos a la salud, esta Tesis ha clasificado los siguientes soportes en donde se ubican los datos que

van a ser tratados o datos para tratamiento: historia clínica, receta y tarjeta sanitaria, a los cuales le añade la actividad de investigación.

El Reglamento (UE) 2016/679 no habla explícitamente del responsable de tratamiento de datos en establecimientos que tratan datos relativos a la salud, sino que es a través del articulado relativo a los delegados de protección de datos que se detecta la significación del responsable de este tipo de tratamientos en el RGPD frente a los demás responsables. Nótese que es el responsable del tratamiento de datos el que nombra al delegado de protección de datos, así pues, a través del estudio de este último podremos deducir la naturaleza del primero.

El artículo 37 del Reglamento (UE) 2016/679 dice que deberá ser nombrado un delgado de protección de datos por el responsable o encargado de una organización en la cual las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9. En consecuencia, el responsable del tratamiento de un establecimiento sometido al artículo 9 deberá en todo caso nombrar a un delegado de protección de datos.

En cuanto a la historia clínica, la Ley 41/2002 establece la jerarquía de responsable del tratamiento o del fichero de la historia clínica. En el artículo 17.4 se establece que la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas son las unidades responsables de la gestión de las historias clínicas en los pacientes hospitalizados, pero que, sin embargo, la custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.

En consecuencia, los responsables del tratamiento de las historias clínicas son los gerentes de los centros sanitarios y los departamentos de admisión y documentación clínica son los encargados de su gestión. Aunque cuando la documentación clínica es utilizada por un facultativo de forma individual en su consulta o clínica particular, el responsable es el facultativo, artículo 17.5 de la Ley 41/2002.

La historia clínica es un documento complejo, del cual se hace cargo en su elaboración y captura de datos el facultativo u otros profesionales de la salud, en consecuencia, el artículo 15.3 dice que "la cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella" a lo que el artículo 17.3 añade que "estos tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes."

Por otra parte, en cuanto a la receta, el otro documento que soporta datos relativos a la salud de la persona tiene dos responsables, el médico y odontólogo, en el momento de expedir la receta y el farmacéutico de la oficina de farmacia, a la hora de dispensar el fármaco y a la hora de destruir, mantener y custodiar la receta médica[581]. De igual forma ocurre con la orden de dispensación de enfermería, en la cual el responsable de la prescripción es el profesional de enfermería o de podología. El hecho de que haya dos

[581] *Vid. Supra pp 346, 348, 354* ,capítulos 3.2.4.1., 3.2.4.2., y 3.2.4.4., del Título III.

responsables de la receta no implica que compartan la corresponsabilidad del artículo 26 del Reglamento (UE) 2016/679, dado que son dos responsabilidades distintas, aunque sobre un mismo documento o conjunto de datos.

En cuanto a la tarjeta sanitaria el responsable de la gestión de los datos incluidos en la tarjeta sanitaria es, por una parte, el responsable del centro sanitario en donde las personas encargadas, empleados o funcionarios utilizan la tarjeta sanitaria para identificar a la persona en el momento requerido o necesario y a los responsables de los centros o instituciones públicas que se encargan de tratar los datos que suministran la tarjeta sanitara en las Bases de Datos de Población Protegía. Este escenario, la tarjeta sanitaria individual del SNS, presenta uno de los supuestos posibles contemplados en el artículo 26, sobre corresponsables del tratamiento, del Reglamento (UE) 2016/679, en cuanto a los corresponsables del tratamiento de los datos.

El fin de cada uno de los tratamientos de datos enmarca a cada escenario en el sector público, en el sector privado o en ambos sectores. La historia clínica representa un escenario de datos utilizado en ambos sectores, sin diferencia entre uno y otro. La receta, también se da en los dos sectores, las recetas se emiten tanto en el sector privado de la salud como en el sector público o sanidad pública. La tarjeta sanitaria Individual, es un escenario de tratamiento de datos personales relativos a la salud tanto en el del Sistema Nacional de Salud como en la sanidad privada.

El responsable del tratamiento de datos relativos a la salud es el responsable de la actividad que genera la organización que utiliza los datos. De tal forma que el responsable del tratamiento de la historia clínica es la persona que ejerce las máximas funciones organizativas del centro en el que se utilizan los datos, por ejemplo, el director gerente de un hospital o clínica. El responsable de la receta es el médico que la prescribe y el farmacéutico de la oficina de farmacia que la dispensa.

El responsable del tratamiento de la tarjeta sanitaria es todo directivo de cualquier organización que utiliza para llevar a cabo su actividad corriente el tratamiento de los datos de las tarjetas sanitarias, en cualquiera de sus formas, es decir, por ejemplo los directores de los hospitales o los responsables de los centros de atención sanitaria en general y los responsables de las Administraciones Públicas o en las empresas privadas encargadas del mantenimiento de las Bases de Datos de Población Protegida del Sistema Nacional de Salud o de las bases de los asegurados en las compañías privadas.

Las personas que suministren sus datos personales a las organizaciones o personas que los necesiten para el ejercicio de su actividad tendrán derecho a conocer la identidad y los datos de contacto del responsable y, en su caso, de su representante, artículo 13.1 del Reglamento (UE) 2016/679.

Cualquier persona, paciente o usuario del sistema sanitario público, de un centro de asistencia sanitaria privado o de una compañía aseguradora de seguros de salud tendrá derecho a conocer los datos de contacto del responsable de sus datos personales.

5.1.1. En el sector público

La norma no distingue entre sector público o sector privado al definir al responsable, de forma explícita, sin embargo, parece que la interpretación de ciertos artículos del Reglamento (UE) 2016/679 permite esta diferenciación. A criterio de la Agencia Española de Protección de Datos, ciertas "cláusulas comodín" o cláusulas que excepcionar la regla, también lo permiten.

En realidad, el fin de los datos, su naturaleza y fin del tratamiento al cual los someten es lo que debe definir al responsable. El Considerando 22 del Reglamento (UE) dice en este sentido, que un establecimiento, el cual tiene un responsable o un encargado, "implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto."

Por otra parte, la lectura detallada del Reglamento (UE) 2016/679 permite acercarse a la figura del responsable del tratamiento de datos a través del delegado de protección de datos, pues este último es nombrado y centrado por el primero.

De esta forma, en primer lugar, el artículo 37 del Reglamento (UE) 2016/679 menciona de forma explícita, nombra y distingue a los organismos públicos como establecimientos en los que el responsable o el encargado del tratamiento deben, en todo caso, nombrar a un delegado de protección de datos.

Por otra parte, este artículo 37, al referirse los responsables del tratamiento distingue a responsables de los organismos públicos y a los responsables de grupos empresariales. En cada caso permite que, si el responsable del tratamiento tiene a su cargo unidades de tratamiento distintas, basta que nombre a un solo delegado de protección de datos.

Esta situación indefinida que planeta el artículo 37 del Reglamento (EU) 2016/679, sin duda plantea problemas a la hora de determinar y concretar en que establecimiento habrá un delegado de protección de datos y en que establecimiento no lo habrá, sino que se compartirá con otro.

Esta situación de indefinición del Reglamento 2016/679, en el sector de la salud, es aclarada por la Ley 0rganica 3/2018 cuando en su artículo 34 determina con muchas más precisión y detalle las organizaciones que deben tener delegado de protección de datos.

Por otra parte, al ser el responsable o el encargado de un tratamiento el que nombrará al delegado de protección de datos , por tanto, al decir que los responsables y encargados del tratamiento deberán designar un delegado de protección de datos cuando se trate de centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes, está indicando, se sobreentiende, que estos centros disponen de un responsable, o como poco de un encargado, obligado al nombramiento de un DPO.

Todos los centros sanitarios que utilicen historias clínicas, recetas o tarjetas sanitarias tienen un responsable del tratamiento de datos, incluso, aunque la organización no lo tenga identificado, pues como dice el artículo 4.y) del Reglamento (UE) 2016/679 hay

un responsable del tratamiento de datos cuando se utilizan datos personales y se tratan, siendo el responsable del tratamiento el que los define y determina los medios para su tratamiento.

El tratamiento de la tarjeta sanitaria no es un escenario específico del sector público. En el sector público, la tarjeta sanitaria individual del SNS, está en uno de los supuestos posibles contemplados en el artículo 26 del Reglamento (UE) 2016/679, en cuanto a los corresponsables del tratamiento de los datos. Esta corresponsabilidad obliga a que todos los corresponsables del tratamiento de la tarjeta sanitaria acuerden sus responsabilidades respectivas. Igual pasa en el caso de las tarjetas sanitarias del sector privado.

Las personas que suministren datos personales a las organizaciones o personas que los necesiten para el ejercicio de su actividad o que estas organizaciones hayan accedido a sus datos sin la intervención de la persona, tendrán derecho a conocer la identidad y los datos de contacto del responsable y, en su caso, de su representante, artículo 13.1 y 14.1 del Reglamento (UE) 2016/679.

En el sector público se incluyen como responsables a todos los directores de los hospitales, a los directores de las Fundaciones de Investigación de los hospitales públicos, a los responsables de los Centros de Atención primaria y a los responsables de las unidades de mantenimiento de las Bases de Datos de Población Protegida del Sistema Nacional de Salud.

5.1.2. En el sector privado

El sector privado no tiene ningún tipo de particularidad en cuanto a la aplicación del RGPD. En ambos sectores la actividad es la misma y los requisitos para llevar a cabo la actividad también son los mismos, lo único que cambia es el soporte que debe llevar la persona para tener acceso al servicio asistencial y las exigencias para el sector público en relación a la designación del DPO, artículo 37.1 RGPD.

La Agencia Española de Protección de Datos es la Autoridad de control principal en España en relación al artículo 51 del Reglamento (EU) 2016/679. Esta Agencia público en el mes de noviembre de 2019 la Guía para pacientes y usuarios de la sanidad.

Esta guía, en el capítulo de legitimación para el tratamiento de datos de la salud, establece una excepción en la necesidad u obligatoriedad del consentimiento del paciente o usuario, afirmando que:

> "no es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para la recogida y utilización de datos personales y de salud si se van a utilizar para fines de medicina preventiva o salud laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social".

El fundamento que utiliza la AEPD es el que se describe a continuación.

La AEPD para realizar tal afirmación acude al artículo 6 del Reglamento (EU) 2016/679, concretamente a sus apartados 6.1.b) y 6.1.c). El apartado 6.1.b) exceptúa la necesidad

de consentimiento cuando 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. El apartado 6.1.c) exceptúa la necesidad de consentimiento cuando el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

A renglón seguido, la AEPD entiende que el apartado 6.1.b) es de aplicación a las compañías aseguradoras de salud privadas y que el apartado 6.1.c) es de aplicación para la sanidad pública.

La aplicación que hace la AEPD del apartado 6.1.b) supone que:

1. El contrato que suscribe una compañía de seguros de salud tiene que ver con la ejecución de un contrato de servicios, lo cual es incierto pues su función está vinculada con la cobertura del pago de los servicios sanitarios que pueda utilizar el cliente en base a su prima.
2. Las compañías de seguros de salud privadas son proveedoras de servicios sanitarios privados, cosa incierta pues la compañía de seguros cubre unas primas no proveen servicios.
3. Las compañías de seguros de salud privadas tienen acceso a los datos de salud de los pacientes o clientes, circunstancia que no se ajusta a la realidad pues ni todas las compañías de seguros tienen centros provisores de servicios propios, ni todos los centros provisores de servicios acogen clientes con pólizas de seguros de salud, ni las compañías de seguros que tienen centros provisores de servicios sanitarios tienen acceso a las bases de datos de los pacientes.

La fortuna o la poca fortuna de la aplicación de esta "cláusula comodín" del Reglamento (UE) 2016/679 para la no aplicación de una o varios principios o normas de protección indica que el RGPD permite interpretar diferencias entre el sector público y el privado.

En cuanto a la aplicación que hace la AEPD del apartado 6.1.c) supone que el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento es solo aplicable a los hospitales públicos y no a los centros privados. Pero lo cierto, es que las obligaciones legales para el responsable de la historia clínica y la receta en un centro público o privado son las mismas.

En este orden de cosas, se entiende que podría ser de aplicación, tanto en el sector público como en el privado, la "cláusula comodín" que permite levantar la prohibición del tratamiento de los datos relativos a la salud sin contar con el consentimiento de la persona y que se haya en el apartado 2 letra h) del artículo 9. Sin embargo, esta "cláusula comodín" no implica que la exceptuación del consentimiento es aplicable a todos los elementos del tratamiento (elementos básicos, complementarios, adicionales y otros, del capítulo 3.2. del Título III), ni que no se deba informar a la persona del tratamiento de sus datos tal como así lo indican los artículos 12, 13 y 14 del Reglamento (EU) 2016/679.

Las normas de aplicación del RGPD para el sector privado son las mismas que para el sector público e incumben de igual forma a los farmacéuticos titulares de las oficinas de farmacia.

Tal vez el sector privado goce de más sencillez a la hora de determinar el responsable del tratamiento de datos y también es más sencillo identificar el establecimiento principal, en casi todos los casos es fácil acudir a las funciones de responsables en las compañías privadas a través de sus contratos. En el caso de las instituciones públicas, en muchas ocasiones no constan de personalidad jurídica propia, lo cual puede dificultar la determinación del establecimiento principal o del responsable legal.

Nota Crítica: la Guía para pacientes y usuarios de la sanidad introduce una excepción a la obligación de consentimiento sobre la cual este capítulo 5.1.2 del Título III discrepa ampliamente. Esta discrepancia ya ha aparecido en el capítulo 3.2 del Título III.

5.2. El encargado del tratamiento de datos en el sector de la salud

El Reglamento (UE) 2016/679 define en su artículo 4.8 al encargado del tratamiento diciendo que "encargado del tratamiento o encargado es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento."

El responsable del tratamiento podrá contratar a una tercera persona que por su cuenta realice el tratamiento de los datos que su establecimiento y actividad requieran. El responsable podrá solo contratar a un solo encargado de un tipo de tratamiento.

El encargado deberá ofrecer al responsable las suficientes garantías de conocimiento para estar en disposición de aplicar las suficientes medidas técnicas y organizativas de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado, artículo 28.1 del Reglamento (UE) 2016/679.

Un encargado no podrá ser contratado por otro encargado sin la autorización previa y por escrito del responsable, artículo 28.2 del Reglamento (UE) 2016/679.

Entre el responsable y el encargado mediará un contrato en el cual se especificarán las funciones, obligaciones y facultades del encargado para llevar a cabo el tratamiento del cual es responsable la parte que le contrata.

El encargado de tratamientos de datos de los datos relativos a la salud de las personas no registro ninguna diferencia en relación a otros tratamientos o a otros datos que no sean de aplicación al responsable del tratamiento.

5.2.1. En el sector público

El encargado, los requisitos para su contratación, sus funciones y obligaciones no se distinguen entre el sector privado y el sector público.

5.2.2. En el sector privado

El encargado, los requisitos para su contratación, sus funciones y obligaciones no se distinguen entre el sector privado y el sector público.

Capítulo 6. El delegado de protección de datos en el sector de la salud

6.1. El delegado de protección de datos (DPO) en la sanidad

El delegado de protección de datos (en adelante, también DPO) es el garante del cumplimiento de la normativa de protección de datos en las organizaciones, garante interno, sin sustituir las funciones que desarrolla la Autoridad de control[582], como garante externo.

El DPO no debe necesariamente ser un jurista, pero los mecanismos voluntarios de certificación que particularmente tienen en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos, artículo 35 de la Ley Orgánica 3/2018.

El sector sanitario, entendido generalmente que sanidad corresponde a un campo de la actividad social, profesional y de servicios cuyo fin es el cuidado de la salud de las personas, en consecuencia, en el sector sanitario el tratamiento de los datos personales relativos a la salud cumple el fin de la actividad de estas organizaciones.

Cualquier responsable del tratamiento de datos podrá nombrar y contratar voluntariamente a un delegado de protección de datos, artículo 37.4 del Reglamento (UE) 2016/679. Pero, en algunos casos habrá responsable del tratamiento obligado a hacerlo.

Estarán obligados al nombramiento de un delegado de protección de datos, en base al Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, el responsable y el encargado de organizaciones siempre que sus actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9.

La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente, en el caso de España se comunica a la Agencia Española de Protección de Datos en un plazo de diez días después de su nombramiento[583].

Lo anteriormente planteado indica que un centro sanitario es siempre subsidiario de disponer de delegado de protección de datos. Sin embargo, se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual, artículo 34.1.l) de la Ley Orgánica 3/2018.

La existencia del DPO es un elemento nuclear en el desarrollo de la nueva normativa sobre protección de datos, más cuando en los centros sanitarios no tan solo el usuario

[582] AEPD (2018) "¿Qué es un delegado de protección de datos?" Diciembre 2018. Disponible en https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-un-delegado-de-proteccion-de-datos (31/01/2021).

[583] AEPD (2021) "Persona delegada en protección de datos". 30 de marzo de 2021. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/persona-delegada-en-proteccion-de (30/04/2021).

o paciente necesita apoyo y asesoramiento, sino que el profesional de la salud tiene que poder contar con personal experto que le asesore convenientemente en estos aspectos.

Por otra parte, el artículo 34.1.I) de la Ley Orgánica 3/2018 es muy claro al determinar, sin salvedades, que deberán tener delegado de protección de datos "Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes".

De tal forma, bien sea por el artículo 37.1 del Reglamento (UE) 2016/679, bien sea por el análisis de las figuras de responsable y encargado del tratamiento de datos o bien sea por el contenido explícito del artículo 34.1.I) de la Ley Orgánica 3/2018, todo ello en su conjunto nos lleva a entender que en cada centro asistencial deberá haber un delegado de protección de datos o alguien que haga sus funciones, en las condiciones que indican tanto el Reglamento (UE) 2016/679 como la Ley Orgánica 3/2018.

Esta obligación de la designación viene reflejada en el artículo 73 sobre infracciones graves del Título IX sobre el régimen sancionador de la Ley Orgánica 3/2018, en cuanto a su incumplimiento. El artículo 73 dice: "El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica". La falta de publicación de los datos del delegado de protección de datos se considera infracción leve. El artículo 74.p) de la Ley orgánica 3/2018 dice al respecto:

> No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

Las sanciones de las infracciones se rigen por el artículo 76 de la Ley Orgánica 3/2018 y por los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679.

El papel del DPO en la sanidad viene determinado por el tipo de datos sometidos a tratamientos por la propia actividad del establecimiento.

El responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales cuando haya riesgo de afectar a los derechos y libertades de las personas que el RGPD quiere proteger. El tratamiento de datos personales relativos a la salud es un tipo de tratamiento que sin duda entraña riesgos especiales y por este motivo el artículo 9 prohíbe su tratamiento, artículo 35.1 del Reglamento (UE) 2016/679.

En el proceso de la evaluación de impacto que tendrá que realizar o encargar el responsable del tratamiento, nótese que no incluye al encargado, el DPO actuará a petición del responsable como asesor del proceso de evaluación, artículo 35.2 del Reglamento (UE) 2016/679.

6.1.1. En el sector público

Ya se ha visto en el apartado anterior que los centros sanitarios en los cuales haya historias clínicas están obligados a tener un DPO y también se entiende en esta Tesis

doctoral, que están obligados a disponer de un DPO los centros que manejen recetas y tarjetas sanitarias individuales.

El RGPD obliga al sector público a tomar medidas más exigentes en el caso de la designación del delegado de protección de datos, artículo 37.1.a) del Reglamento (UE) 2016/679.

Por otra parte, el artículo 37.3 del Reglamento 206/679 dice "cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura y tamaño". Lo cual en una primera lectura genera dudas sobre si la Administración pública debe designar un delegado de protección de datos en cada uno de sus centros sanitarios que dependan o estén adscritos al mismo o si bien puede designar un único DPO que se ocupe del tratamiento de datos de todos los centros conjuntamente. Esa aclaración obliga a dos análisis previos, por una parte, al análisis de las figuras del responsable y del encargado del tratamiento de los datos, dado que el delegado de protección de datos es designado por uno de ellos y, por otra parte, estudiar el trato que hace la Ley Orgánica 3 /2018 de los centros sanitarios en su artículo 34.1.

Una primera lectura del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, parece indicar que el responsable del tratamiento es el titular del centro sanitario o el que tiene encomendado legalmente su fin y su misión, en términos generales podemos referirnos que el máximo responsable de los Organismo Públicos con personalidad jurídica propia son los responsables del tratamiento de los centros asistenciales bajo su dependencia, salvo los centros sanitario o establecimientos sanitarios públicos que no tienen personalidad jurídica propia, en cuyo caso el responsable es el máximo órgano de la organización. Mientras que, en este último supuesto, en el máximo directivo del centro asistencial recae la figura del encargado del tratamiento, es decir, sobre el Director Gerente de cada centro sanitario.

Sin embargo, la ubicación del responsable del tratamiento de datos en la sanidad pública no parece tan clara cuando se analiza el máximo desempeño y obligación del responsable del tratamiento de datos en el entorno sanitario, sin duda a nadie se le escapa que es el tratamiento de la historia clínica, la recta y la tarjeta sanitaria.

Sin entrar en análisis innecesario de la cuestión la simple lectura del artículo 14, definición y archivo de la historia clínica, Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, ubica al responsable del tratamiento de los datos en centros donde sea necesaria la elaboración y utilización de historias clínicas en el propio centro que las genera, las crea, las custodia y las utiliza.

Por otra parte, el artículo 34.1.I) de la Ley Orgánica 3/2018 es muy claro al determinar, sin salvedades, que deberán tener delegado de protección de datos "Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes".

De tal forma, bien sea por el artículo 37.1 del Reglamento (UE) 2016/679, bien sea por el análisis de las figuras de responsable y encargado del tratamiento de datos o bien sea por el contenido explícito del artículo 34.1I) de la Ley Orgánica 3/2018, todo ello en su conjunto nos lleva a entender que en cada centro asistencial deberá haber un DPO o alguien que haga sus funciones, en las condiciones que indica tanto el Reglamento (UE) 2016/679 como la Ley Orgánica 3/2018.

Es evidente que el Reglamento (UE) 2016/679 cuando, en su artículo 37.3, hace referencia al organismo público no incluye al organismo público de sanidad excluido por el artículo 34.1I) de la Ley Orgánica 3/2018 que actúa como una normativa nacional que sin restar objeto y ámbito a la ley refuerza las exigencias de unos de sus preceptos.

Resumiendo, aunque el Reglamento (UE) 2016/679 en su artículo 37.3 entiende que cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único DPO para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño, lo cierto es que, el artículo 34.1.I) de la Ley orgánica 3/2018 estipula claramente que los responsables y encargados del tratamiento deberán designar un DPO en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

La no designación de delegado de protección de datos es una infracción considerada grave por la Ley Orgánica 3/2018, artículo 73.v). La AEPD mediante la resolución de 9 de junio de 2020 impuso multa por infracción grave a la empresa GLOVOAPP23, S.L. por no nombrar a un delegado de protección de datos[584], a pesar de disponer de un Comité de Protección de datos[585].

Por otra parte, si se entiende que el responsable del tratamiento de datos en la sanidad pública es el máximo responsable de cada uno de los centros sanitarios públicos, entonces en este supuesto el DPO debería estar ubicado en cada uno de los centros sanitarios.

6.1.2. En el sector privado

Nada dice el RGPD que distinga el tratamiento del dato en la actividad sanitaria del sector privado, tan solo obliga al sector público a tomar medidas más exigentes como en el caso de la designación del delegado de protección de datos, artículo 37.1.a) del Reglamento (UE) 2016/679.

El Reglamento (UE) 2016/679 en su artículo 37, se refiere directamente al sector sanitario en su apartado 1.c) al referirse a su artículo 9. De esta forma al referirse en el apartado 1.a) al sector público en general, se sobreentiende que el apartado 1 en su conjunto se refiere a todos los sectores, al público y al privado.

Aun así, el apartado 1.c) del artículo 37 añade: “en el tratamiento a gran escala”. Esta matización excluye los tratamientos a pequeña escala. Podría servir de referencia la

[584] AEPD (2020). Resolución de la Agencia Española de Protección de Datos PS/00417/2019, de 9 de junio de 2020
[585] *Vid. Infra p 420,* capítulo 6.3., del Título III.

excepción que realiza el artículo 30 del Reglamento (UE) 2016/679 a la obligación de llevar registro de actividades, cuando en su apartado 5, a las empresas de menos de 250 empleados, si no fuera porque el mismo apartado excluye a las organizaciones incluidas en el artículo 9.

A falta de más concreción, parece conveniente acudir a los usos en el sector sanitario en base a los cuales podría considerarse pequeña escala a la actividad profesional privada llevada a cabo por un profesional sanitario. De esta forma, el Reglamento está haciendo mención de que tan solo las organizaciones sanitarias en donde trabajan profesionales de la salud por cuenta ajena están obligadas a nombrar y contratar un DPO.

En este orden de cosas, la Ley Orgánica 3/2018 en su artículo 34 viene a expresar lo mismo que el Reglamento (UE) 2016/679 en relación a la escala del volumen de tratamiento de datos, al excluir a los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

Nada dice el Reglamento (UE) 2016/679 ni la Ley Orgánica 3/2018 de las oficinas de farmacia, que si bien no están obligadas el mantenimiento de historias clínicas utilizan la tarjeta sanitaria del paciente y tienen acceso a las recetas de los pacientes.

El artículo 1 de la Ley 16/1997, de 25 de abril, de regulación de servicios de las oficinas de farmacia define a las oficinas de farmacia se definen como establecimientos sanitarios privados de interés público. En base al artículo 9 del Reglamento (UE) 2016/679 la Oficina de Farmacia está sujeta al RGPG, pero al no tratar datos a gran escala parece que no estaría obligada a disponer de DPO[586].

Por otra parte, el artículo 34 de la Ley orgánica 3/2018 incluye a toda organización que mantenga historias clínicas y si bien las oficinas de farmacia no mantienen historias clínicas, utilizan la tarjeta sanitaria del paciente lo cual da la posibilidad a que la Oficina de Farmacia pudiera acceder a los datos de la historia clínica de la persona.

La no designación de delegado de protección de datos es una infracción considerada grave por la Ley Orgánica 3/2018.

Así pues, en base al principio de integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados, artículo 25 del Reglamento (UE) 2016/679, al principio de proactividad, artículo 5.2 del Reglamento (UE) 2016/679, que impulsa el RGPD y en base a la libertad de designación de PDO, artículo 37.4 del Reglamento (UE) 2016/679, en supuestos no obligados, se entiende que las oficinas de farmacia deberían disponer[587], es decir,

[586] COMISIÓN EUROPEA. "Directrices sobre los delegados de protección de datos (DPO)". Adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017. Grupo de trabajo sobre protección de datos del artículo 29. Disponible en https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf (28/02/2021)

[587] GASULLA, A. (2018) "El Reglamento Europeo de Protección de Datos y las oficinas de farmacia". Aula Farmacia. Disponible en http://www.auladelafarmacia.com/articulo/gestion/reglamento-europeo-proteccion-datos-oficinas-farmacia/20181112111247002519.html (30/04/2021)

contratar los servicios de un DPO aunque fuera a tiempo parcial, comunicándolo a la AEPD. Este apoyo de un delegado de protección de datos se hace más patente en cuanto que el consentimiento de la persona para que la farmacia pueda tratar los datos de las recetas privadas no electrónicas, no está claro. Sin duda esta cuestión requiere no tan solo el apoyo de un DPO sino el pronunciamiento de la AEPD.

6.2. El delegado de protección de datos en el sector de la sanidad, en base al Reglamento (UE) 2016/679 y su reflejo en la Ley orgánica 3/2018

El Reglamento (UE) 2016/679 alude a los datos relativos a la salud en su Considerando 35 entendiendo como dato relativo a la salud a cualquier dato que de información sobre su organismo y a cualquier dato personal recogido como consecuencia de su inscripción en una organización sanitaria para su asistencia o como consecuencia de la propia asistencia, remitiéndose a la Directiva 2011/24/UE del Parlamento Europeo y del Consejo.

El Considerando 35 añade además que será considerado dato relativo todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios.

A todo ello el Considerando 35 incluye, como es obvio, la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

Los datos relativos a la salud aparecen en el Reglamento (UE) 2016/679 en el artículo 9 titulado Tratamiento de categorías especiales de datos personales. El apartado 1 del artículo 9 prohíbe el tratamiento de los datos relativos a la salud.

En este orden de cosas, serán establecimientos incluidos dentro de este artículo 9 aquellos que para la realización de su actividad principal es preciso el tratamiento de datos personales relativos al Considerando 35 del Reglamento (UE) 2016/679.

La Ley orgánica 3/2018 aborda los datos de la salud por otra vía. En su Título II sobre los principios de la protección de datos incluye en el artículo 9 lo que viene a llamar las categorías especiales de datos.

Por otra parte, el Reglamento (UE) 2016/679 establece unas determinadas obligaciones para los responsables y encargados del tratamiento de datos. Una de estas obligaciones es la designación y contratación de un delegado de protección de datos. Así pues, una cuestión de suma importancia se centra en determinar en qué establecimientos debe nombrarse a un DPO o contratar sus servicios.

En cuanto al nombramiento del DPO, si bien es cierto que el Reglamento (UE) 2016/679 en su artículo 37.3 genera imprecisión en el sector público al decir que las entidades públicas

podrán asignar un único DPO para varios organismos, también lo es que la Ley Orgánica 3/2018 corrige esta laguna y su artículo 34.1 aporta más claridad y concisión al decir:

> "Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:
>
> l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
>
> Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual."

El Reglamento (UE) 2016/679 nada dice en relación con la receta y a la tarjeta sanitaria individual ni a la tarjeta sanitaria europea, sin embargo, de su lectura se extrae, especialmente de su Considerando 35, que tanto en un caso como en otro se incluyen en el artículo 9 del Reglamento (UE) 2016/679.

Por una parte, las oficinas de farmacia, en base al artículo 37 Reglamento (UE) 2016/679, no estarán obligadas a tener un DPO, pero que, por los principios de garantías necesarias y el principio de protección de los interesados, artículo 25 del Reglamento (UE) 2016/679, y por el principio de proactividad, artículo 5.2 del Reglamento (UE) 2016/679, se puede deducir que deberían disponer de un DPO[588].

En cuanto a las tarjetas sanitarias, todos los centros en donde se traten estos datos deberían tener un DPO, en el caso de los centros pequeños, se les aplicaría lo dicho para las oficinas de farmacia y en el caso de las compañías de seguros con Bases de Datos de asegurados y en los centros con Bases de Datos de Población Protegida del SNS, deberían disponer de DPO, en todo caso.

El Reglamento (UE) 2016/679 incluye el tratamiento de datos personales relativos a la salud dentro del artículo 9. En consecuencia, cuando los centros de investigación tengan una actividad a gran escala, en base al artículo 37.1.c) del Reglamento (UE) 2016/679, deberán disponer de DPO.

En España el RGPD es más concreto y la Disposición adicional decimoséptima, sobre tratamientos de datos de salud, en su apartado 2, letra h) estipula que, a partir del 6 de diciembre de 2019, los comités de ética en el ámbito de la investigación de la salud, biomédico o del medicamento, deberán disponer de un DPO y este deberá ser miembro del comité. En el caso de que no fuera posible, deberá contar con un experto en el Reglamento (UE) 2016/679. Esta condición se aplicará tanto si el centro de investigación trata datos personales como datos seudonimizados o datos anonimizados.

[588] GASULLA, A. (2018) "El Reglamento Europeo …..", op.cit;

6.3. La figura del delegado de protección de datos y su aplicación en la sanidad pública. El supuesto de la Consejería de Sanidad de la Comunidad de Madrid

Desde el punto de vista organizativo el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 obliga al nombramiento de un delegado protección de datos en determinadas circunstancias y supuestos.

Esta obligación se manifiesta de forma más explícita cuando se trata de un organismo público, de tal forma el artículo 37.1 del Reglamento (UE) 2016/679 estipula que el responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que el tratamiento lo lleve a cabo una autoridad u organismo público y cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9.

Todo esto indica que un centro sanitario público es subsidiario de disponer de delegado de protección de datos.

La existencia del DPO es un elemento nuclear en el desarrollo de la nueva normativa sobre protección de datos, más cuando en los centros sanitarios no tan solo el usuario o paciente necesita apoyo y asesoramiento, sino que el profesional de la salud tiene que poder contar con personal experto que le asesore convenientemente en estos aspectos.

Sin embargo, por otra parte, esta obligación del artículo 37.1 se matiza y flexibiliza en el artículo 37.3 del Reglamento 206/679 cuando permite que un organismo púbico nombre a un mismo DPO para varios organismos, expresándolo mediante este párrafo “cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura y tamaño”.

Esta obligación con salvedades, en una primera lectura genera dudas sobre si un Servicio Regional de Salud debe designar un DPO en cada uno de los centros sanitarios que dependan o estén adscritos al mismo o si bien puede designar un único DPO que se ocupe del tratamiento de datos de todos los centros sanitarios conjuntamente.

Esa aclaración obliga a los análisis previos, el primero de ellos, al análisis de las figuras del responsable y del encargado del tratamiento de los datos, para conocer en dónde se ubica el obligado, dado que el DPO es designado por uno de ellos y, por otra parte, estudiar en qué manera aborda la designación de DPO la Ley Orgánica 3 /2018 y si hace alguna mención a los centros sanitarios.

Una lectura detenida del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, parece indicar que el responsable del tratamiento es el titular del centro sanitario o el que tiene encomendado legalmente su fin y su misión, en donde reside la persona jurídica con plena capacidad de obrar. En términos generales y bajo un punto de vista organizativo dentro de la Administración pública sanitaria, podría entenderse que el máximo responsable de los Servicios Regionales de Salud (en adelante también, SRS) es el responsable del tratamiento de los centros asistenciales bajo su dependencia, excepto

los que tiene personalidad jurídica propia en cuyo caso el responsable es el máximo órgano de la organización. Siguiendo con esta argumentación, se entendería entonces que el máximo directivo del centro asistencial recaería la figura del encargado del tratamiento, es decir, sobre el director gerente de cada centro sanitario. En base a esta argumentación el DPO podría ser nombrado tanto por el máximo responsable del Servicio Regional de Salud como por el director del centro. Si embargo, persistiría la duda sobre si es posible que haya un solo DPO para todos los hospitales o debería haber uno en cada hospital, con independencia de quien lo nombrara.

Por otra parte, si se aborda la cuestión definiendo el establecimiento principal como el establecimiento en donde se realiza el tratamiento de los datos que cubren el fin de la propia organización que los genera, entonces en este caso, el centro principal no se identifica con el que tiene personalidad jurídica propia sino con el establecimiento en el que se realiza el tratamiento de los datos personales, y estos establecimientos son sin duda los centros sanitarios. Si, por otra parte, nos dirigimos a consultar la legislación complementaria que regula la historia clínica como la base de datos de la actividad generada en la organización, y esta norma determina que el responsable del tratamiento de la historia clínica es el director del centro sanitario, así pues, en base a todo ello el responsable del tratamiento no es máximo responsable del SRS sino el máximo responsable del centro asistencial, es el director gerente o director general del mismo.

En base a la argumentación del párrafo anterior, el responsable del tratamiento de datos personales relativos a la salud es el máximo responsable del centro sanitario y en consecuencia cada centro sanitario deberá disponer de un DPO.

Abandonando la lectura del Reglamento (UE) 2016/679 y abordando el texto de la Ley Orgánica 3/2018, nos encontramos con una aplicación más clara de la obligación de nombrar a un DPO en el sector de la sanidad.

El artículo 34.1.l) de la Ley Orgánica 3/2018 es muy expeditivo al determinar, sin salvedades, que deberán tener delegado de protección de datos “Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes”.

De tal forma, bien sea por el artículo 37.1 del Reglamento (UE) 2016/679 y por el análisis de las figuras de responsable y encargado del tratamiento de datos o bien sea por el contenido explícito del artículo 34.1.l) de la Ley Orgánica 3/2018, todo ello en su conjunto nos lleva a entender que en cada centro asistencial deberá haber un DPO o alguien que haga sus funciones, en las condiciones que indica tanto el Reglamento (UE) 2016/679 como en la Ley Orgánica 3/2018.

Resumiendo, el Reglamento (UE) 2016/679 en su artículo 37.3 entiende que cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único DPO para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño, sin embargo, el artículo 34.1.l) estipula que los responsables y encargados del tratamiento deberán designar un DPO en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso,

cuando se trate de centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Por otra parte, es evidente que el Reglamento (UE) 2016/679 cuando, en su artículo 37.3, hace referencia al organismo público no incluye al organismo público de sanidad excluido por el artículo 34.1.I) de la Ley Orgánica 3/2018, actuando esta como una normativa nacional que sin restar objeto y ámbito al Reglamento (UE) refuerza e incrementa las exigencias de unos de sus preceptos.

El resultado de observar la forma en que la Administración Pública, o parte de ella, ha resuelto la exigencia de artículos 37, 38 y 39 del Reglamento (UE) 2016/679 y artículos 34, 35 y 36 de la Ley Orgánica 3/2018 y en concreto la exigencia del punto 1.I) del artículo 34, artículo 34 de la Ley Orgánica 3/2018, con relación al DPO a fecha de 1 de abril de 2021 nos hace pensar que no han sabido resolver sus dudas, que aún persisten.

Por poner un ejemplo, la Viceconsejería de Sanidad de la Comunidad de Madrid comunica el día 27 de abril de 2018 a la Agencia Española de Protección de Datos la creación de una figura colegiada denominada Comité delegado de protección de datos (Anexo LL). Esta figura colegiada, atípica, no consta en el Reglamento (UE) 2016/679 ni en la Ley Orgánica 3/2018 e implica y arrastra todo el desarrollo normativo que necesita la propia normativa de protección de datos, pues difícilmente se podrá conciliar esta acción administrativa con las figuras, obligaciones y responsabilidades del responsable y del encargado del tratamiento en los centros sanitarios públicos, tal como veremos en adelante.

La creación de una figura colegiada del delegado de protección de datos no tan solo es sorprende por atípica por no estar amparada por ni la Ley Orgánica 3/2018 ni por el Reglamento (UE) 2016/679 en dos extremos. El primero, ubica artificialmente al responsable del tratamiento de los historias clínicas, tarjetas sanitarias públicas y recetas emitidas por los profesionales del Servicio Madrileño de Salid en la figura del Consejero, circunstancia no amparada ni por la norma ni por el normal funcionamiento del sector público de la sanidad ni por el sentido común de las cosas. El segundo, sorprende, más si cabe, el amparo al que se acoge el comunicado de la Viceconsejería de Sanidad.

La creación del Comité delegado de Protección de Datos se ampara en el Comité de Seguridad de la Información de la CSM, en virtud de las competencias de la Orden 491/2013, de 27 de junio, de la Consejería de Sanidad, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica, obviando y omitiendo, al parecer, que el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 no excluyen, ni muchos menos, a los datos y a la información que están soportados en documentos de papel, gráficos, en imágenes y en sonidos y que nada tienen que ver con los sistemas informáticos. Con esta justificación la Viceconsejería parece que reinterpreta el Reglamento (UE) 2016/679, posicionándolo tan solo como legislación relativa al tratamiento de datos informáticos.

Es preciso hacer notar que la AEPD mediante la resolución PS/00417/2019 de 9 de junio de 2020 sancionó a la empresa GLOVOAPP23, S.L. por infracción graves por no disponer

de delegado de protección de datos a pesar de que la empresa alega disponer de un Comité de Protección de datos[589].

Según se deduce de la web de la AEPD, a fecha de mayo de 2021, que debe publicitar a los delegados de protección de datos nombrados y comunicados a las Agencias, que es generalizada en todas las Comunidades Autónomas la ausencia de delegados de protección de datos en los centros provisores de servicios sanitarios públicos, en los centros de datos de las tarjetas sanitarias y en muchos centros de investigación[590].

En toda esta argumentación, se ha utilizado la historia clínica como máximo referente de las bases de datos relativos a la salud de las personas, pero como ya se ha sostenido en todo el texto de la Tesis, también se hace extensivo al uso de la tarjeta sanitaria y al uso de la receta.

[589] AEPD (2020). Resolución de la Agencia Española de Protección de Datos PS/00417/2019, de 9 de junio de 2020. p 2.

[590] AEPD (2021) "Consulta DPD" Disponible en https://sedeagpd.gob.es/ sede-electronica-web /vistas/ infoSede/ consultaDPD.jsf (30/04/2021).

TÍTULO IV. EL DELEGADO DE PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO DE LA SANIDAD

Capítulo.1. La identificación de responsables del tratamiento de datos en el sector público de la salud

El Reglamento General de Protección de Datos regulado por el Reglamento (UE) 2016/679 y en España, por la Ley orgánica 3/2018 introducen una serie de innovaciones en el ordenamiento jurídico y en la forma de velar por los derechos de las personas relacionados con la protección de sus datos y, en consecuencia, de su intimidad.

La identificación correcta del responsable del tratamiento es una de las premisas de la protección de los datos de las personas, además también es una forma para evitar lo que ha ocurrido en la sanidad pública de toda España[591] y en concreto en la Comunidad de Madrid en relación con la aplicación del Reglamento (UE) 2016/679 y la Ley orgánica 3/2018 en la sanidad pública.

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento, artículo 24.1 del Reglamento (UE) 2016/679. El responsable del tratamiento es el primer eslabón dentro de la escala de la aplicación del RGPD básicamente en relación a la definición de tratamiento del artículo 4.2 del Reglamento 2016/679 y más concretamente en lo que hace referencia a la recopilación, administración, mantenimiento, utilización, acceso y revocación de los datos personales, debiendo comunicar a la Autoridad de control todas las violaciones del acceso a los datos personales, en un plazo no superior a 72 horas, artículo 33.1 del Reglamento (UE) 2016/679.

El responsable del tratamiento es quien debe aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento, artículo 4.7) del Reglamento (UE) 2016/679, frente a los interesados y ante las autoridades de supervisión, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. Unas medidas se aplicarán en base al nivel y tipo de riesgo de los tratamientos y otras medidas se aplicarán cuando exista un alto riesgo para las libertades y derechos de las personas, tal como expone la AEPD en su guía de septiembre 2019 [592].

El Reglamento (UE) 2016/679 no enumera las medidas que deberá adoptar el responsable en su tarea de garantía de seguridad de los datos personales, sin embargo, por una parte, el artículo 24 menciona dos supuestos, tales son la adhesión a los códigos de conducta y la adhesión a un mecanismo de certificación del artículo 42, y por la otra, la protección de datos desde el diseño y por defecto, artículo 25, en base al principio de

[591] *Vid. Supra p 421*, capítulo 6.3., del Título III.

[592] AEPD (2019) "Guía del Reglamento General de Protección de Datos. Para responsables del tratamiento". Guía de protección de datos UE. Septiembre 2019. Disponible en https://www.aepd.es /sites /default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf (31/01/2021).

proactividad. La otra gran medida en manos del responsable del tratamiento es el nombramiento y/o contratación de un delegado de protección de datos. El DPO es una de las piedras angulares de RGPD, que, si bien no es una figura nueva, pues ya existía en la Directiva 95/46/UE, su obligatoriedad en determinadas situaciones es un elemento novedoso y de gran significado. La obligación recae en el responsable del tratamiento y el también, es su caso, el encargado. Pero como el responsable es el que podrá contratar o no nombrar al encargado del tratamiento, lo inmediato será identificar al responsable del tratamiento.

Para la identificación del responsable del tratamiento de datos en primer lugar hay que determinar a qué tipo de actividad corresponden los datos que se registran y cuál es el fin de dicho registro. La actividad deberá corresponder a una organización, las actividades a pequeña escala, como las que pueden llevar a cabo profesionales que trabajan de forma individual o bien aquellos tratamientos de datos que se llevan a cabo en domicilios particulares, no están en el ámbito de aplicación del Reglamento (UE) 2016/679.

De tal forma, todo tratamiento de datos corresponde a un tipo de actividad principal, dicho de otra forma, para el desarrollo de una actividad principal de una organización hará falta recabar una serie de datos propios de la actividad de esta, a estos datos hace referencia la expresión de "tratamiento de datos".

En muchos casos, se identifica a la organización con la persona jurídica de la misma, lo cual desde el punto de vista mercantil y civil tiene mucho sentido, pero en el ámbito del Reglamento (UE) 2016/7679 no siempre existe esta correlación. Una singularidad en las organizaciones sanitarias que fueron creadas al amparo de la Seguridad Social en España es su falta de personalidad jurídica propia, conformándose como organizaciones burocráticas en base a lo que viene a llamarse gestión indiferenciada[593].

La Ley Orgánica 3/2018, en el apartado 1 letra l) de su artículo 34, sobre designación de un delegado de protección de datos, especifica en el punto l) los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que utilicen historias clínicas de los pacientes, ejerzan su actividad a título individual. Lo cual no genera ningún género de duda en cuanto a los establecimientos que deben ser considerados subsidiarios de que el responsable nombre a un DPO.

Identificar al responsable del tratamiento de datos de las historias clínicas, también de tarjetas sanitarias y recetas, en los centros sanitarios se puede abordar bien directamente mediante un procedo deductivo o bien mediante alguna norma que pueda identificar por si sola al responsable de dicho tratamiento.

[593] GARRIDO FALLA, F. (1992) "Tratado de Derecho Administrativo. Volumen II". Edición 10ª. Madrid. Ed, Tecnos. pp 349-350; y GAMERO CASADO, E. (7 noviembre 2019) "Criterios determinantes de la forma de gestión de los servicios públicos; especial referencia a la remunicipalización de servicios locales". La Administración al día. Instituto Nacional de Administración Pública. Disponible en http://laadministracionaldia.inap.es/noticia.asp?id=1510094 (31/01/2021).

Tal como consta en el capítulo 3.2.2. del Título III, el profesional sanitario que tiene a su cargo coordinar la información y la asistencia sanitaria del paciente o del usuario es el médico responsable, interlocutor principal durante el proceso asistencial, sin perjuicio de las obligaciones de otros profesionales que participan en las actuaciones asistenciales, artículo 3 de la Ley 41/2002. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle, artículo 4.3 de la Ley 41/2002, además de ser responsables de la propia historia clínica[594] . Así pues, el primer nivel de responsabilidad directa recae en el propio médico que confecciona la historia clínica.

Son los centros sanitarios los que adoptaran las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental[595]. De esta forma, cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten, artículo 16.2 de la Ley 41/2002. Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información, artículo 14 de la Ley 41/2002.

La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas[596]. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario, artículo 17.4 de la Ley 41/2002. Así pues, el segundo nivel responsable, o responsable permanente, es el propio centro sanitario.

Hay otro tipo de responsable en lo relativo a la historia clínica, este es la Administración pública sanitaria de la Comunidad Autónoma, artículo 14.4 de la Ley 41/2002. En este orden de cosas el artículo 14 de la Ley 41/2002 dispone que las AAPP de las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental[597]. Así pues, la Administración pública sanitaria se configura como el tercer nivel de responsabilidad. Este caso, la Administración pública sanitaria actuaría como corresponsable del tratamiento de datos, artículo 25 del Reglamento (UE) 2016/679.

Si embargo, a efectos del responsable del tratamiento de los datos integrantes de la historia clínica atendiendo a la definición de tratamiento del artículo 4 del Reglamento (UE) 2016/679, que dice:

[594] STS 3006/2010 de 2 de junio de 2010 (Sala de lo Contencioso), FD 1º.
[595] *Vid. Supra p 403*, capítulo 5.1., del Título III.
[596] STS 3006/2010 de 2 de junio de 2010 (Sala de lo Contencioso), FD 1º.
[597] *Vid. Supra p 270*, capítulo 1.2.5.1., del Título III.

> "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción",

El responsable del tratamiento de datos de la historia clínica es la dirección del centro, la cual está representada por la figura del director gerente, denominación frecuente en el sector público, o del director general, denominación frecuente en el sector privado. Lo cual sitúa al médico como un corresponsable del tratamiento de datos, artículo 25 del Reglamento (UE) 2016/679.

La Tesis mantiene que además de la historia clínica, el artículo 9 del Reglamento (UE) 2016/679 hace referencia a la receta. En el capítulo 3.3.3. del Título III se menciona que los datos de la receta nacen cuando se emiten y están íntimamente relacionados con la historia clínica, aunque no forma parte de esta y tiene una naturaleza temporal, nace cuando se emiten los datos en el documento, receta, y su fin se agota al ser dispensado, por el farmacéutico. La receta es pues un documento que tiene dos responsables del tratamiento de estos datos, por una parte, el responsable de la emisión de estos y por otra parte el responsable del tratamiento final de estos[598]. En el caso de la oficina de farmacia el responsable es el farmacéutico titular de la farmacia, artículo 5.3 de la Ley 16/1997.

Otro elemento dentro del tratamiento de los datos relativos a la salud es la tarjeta sanitaria, y dentro del Sistema Nacional de Salud conocida habitualmente como TIS, tarjeta sanitaria individual. En el capítulo 1.2.5.3 del Título III se encuadra el tratamiento de la tarjeta sanitaria dentro de los que contempla el artículo 9 del Reglamento (UE) 2016/679. En el capítulo 1.2.5.3.1.4. del Título III se trata la Base de Datos de Población Protegida del Sistema Nacional de Salud y en el capítulo 1.2.5.3.1.2 del Título III se trata el Código de Identificación Personal, en conexión con la historia clínica tratada en el capítulo 1.2.5.1.1. en cuanto a los Códigos de Identificación de la historia clínica. Esta íntima interconexión entra la tarjeta sanitaria y la historia clínica convierten a la tarjeta sanitaria en un documento del tratamiento de datos relativos a la salud especialmente vulnerable en cuanto a la protección de dichos datos.

Esta vulnerabilidad de los datos relativos a la salud que presenta la tarjeta sanitaria recomienda tanto por el propio artículo 9 del Reglamento 2016/679, como por su gran escala, artículo 37.1.b) del Reglamento (UE) 2016/679, por los principios de garantías necesarias y el principio de protección de los interesados, artículo 25 del Reglamento (UE) 2016/679, y por el principio de proactividad, artículo 5.2 del Reglamento (UE) 2016/679, que se deberían disponer de PDO en todos los puntos de tratamiento de la Base Datos de Población Protegida del Sistema Nacional de Salud del capítulo 1.2.5.3.1.4. del Título III, ubicados en las Administraciones sanitarias, al igual debería hacer las compañías de seguros de salud con sus centros de datos.

[598] *Vid. Supra p 341,* capítulo 3.2.4., del Título III.

En consecuencia, se debe identificar al responsable del tratamiento de los datos de la tarjeta sanitaria en cuanto a la Base de Datos y al responsable del tratamiento de datos de todos los establecimientos en donde se utiliza la tarjeta sanitaria. Así pues, el responsable de la historia clínica y el de la tarjea sanitaria pueden coincidir en los centros obligados al mantenimiento de las historias clínicas de los pacientes, pero también puede haber centros en los que se trate la información de la tarjeta sanitaria y que en el mismo centro no estén obligados al mantenimiento de la historia clínica, aunque si acceso a la historia clínica electrónica, por ejemplo, los centros de Atención primaria.

Una vez detectados los responsables del tratamiento de los datos relativos a la salud de las personas de las organizaciones cuya actividad se sustenta en estos datos y en su tratamiento, se debe analizar si este responsable debe nombrar a un DPO o sin estar obligado a ello es conveniente que lo designe.

Cabe destacar que una misma fuente de datos puede tener varios responsables del tratamiento, tal es el caso de los datos personales relativos a la salud. Por una parte, estos datos van a la historia clínica, por otra parte, a la receta y por otra, a la tarjeta sanitaria, todos ellos con sus tratamientos específicos y destinados a actividades distintas, todos ellos con distintos responsables y en algún caso con corresponsables.

Resumen, pasos a seguir para la identificación del responsable del tratamiento de datos:

1.º Identificar datos y tipos de datos registrados o a registrar.
2.º Identificar tipo de actividad a los que corresponden los datos que se registran y cuál es el fin de dicho registro.
3.º Identificar tipo de tratamiento.
4.º Identificar la organización que hace posible la actividad y que trata los datos.
5.º Identificar los niveles de responsabilidad, bien de forma deductiva o bien acudiendo a la norma, en su caso.
6.º Identificar al responsable del tratamiento de datos o el responsable principal y los corresponsables, en su caso.
7.º Identificar las obligaciones del responsable del tratamiento de datos en base al tipo de datos, tipo de tratamiento, volumen del tratamiento y tamaño de la organización.

Capítulo.2. El delegado de protección de datos en la protección de los principios del RGPD y la aplicación del derecho a la protección de la salud en el sector público de la salud

2.1. El delegado de protección de datos y la protección de los principios de la protección de datos del RGPD que aparecen en el capítulo 2.1. del Título III

En el capítulo 4.1.5. del Título II se dice que del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 se concluye que el delegado de protección de datos (DPO) debe desempeñar sus funciones dentro de las dependencias del centro responsable y que depende del responsable o encargado del tratamiento, sin que, a su vez, esté sometido a las instrucciones de ningún estamento de la organización o compañía, incluyendo al responsable del tratamiento o al encargado, por las condiciones del art. 38 RGDP, puntos 3 y 5.

En el capítulo 6.1.1. del Título III se describe que los centros asistenciales o centros sanitarios que dispongan de historias clínicas, tarjetas sanitarias o recetas están obligados a disponer de un delgado de protección de datos, cuando su tamaño así lo aconseje. En cuanto a la relación del delegado de protección de datos con un posible Comité de Protección de Seguridad de Datos constituido en su centro de trabajo, en base a lo que indica el art. 38 del RGDP, este no podría ser miembro de dicho Comité y en el caso de que el Comité requiera su presencia los hará como invitado con voz, pero sin derecho a voto[599].

El capítulo 4.1.5. del Título II describe las funciones del delegado de protección de datos, artículo 39 RGDP, son el asesoramiento general en todo lo relativo a la protección de datos personales y de las obligaciones que impone el Reglamento (UE) 2016/679 y de otras obligaciones de otras disposiciones de protección de datos de la Unión o de los Estados miembros. En consonancia con ello deberá realizar supervisión y auditorías del cumplimiento del Reglamento (UE) 2016/679 y de otra legislación de protección de datos de aplicación; de las políticas en materia de protección de datos (de privacidad); así como deberá elaborar informes de evaluación de impacto de ciertos tratamientos de datos personales del artículo 35.3.h) del RGDP, los relativos al artículo 9; la cooperación con la Autoridad de control; y actuar como punto de contacto de la Autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar, consultas, en su caso, sobre cualquier otro asunto.

Por otra parte, el capítulo 2 del Título III describe los principios de la protección y del tratamiento de datos en la normativa de protección de datos personales en el sector de la salud.

La conexión de estos capítulos da pie a describir la relación del delegado de protección de datos y la protección de los principios reflejados en el RGPD, en el sector público de la salud o sector público sanitario.

[599] *Vid. Supra p 432*, capítulo 4.1.5., del Título II.

El delegado de protección de datos en cualquier centro sanitario deberá velar por los principios del RGPG en consonancia con la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Estos con carácter general recogen el principio de respeto a la intimidad de las personas y a la digitad humana, al que la Ley 41/2002 suma el de la autonomía de la voluntad[600]. A estos tres principios se les añaden el principio consentimiento de las personas, pacientes o usuarios, y en el sector sanitario, del cumplimiento de los deberes, por parte de los profesionales sanitarios, de información y de documentación clínica y de la reserva debida en relación con estas. En el sector de la salud, se añaden los principios que justifican las obligaciones de los pacientes en materia de datos, de aquí el principio del deber de facilitar datos sobre su salud cuando se reclame la atención o asistencia de esta. De tal forma, los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria, artículo 2.5 de la Ley 41/2002.

El delegado de protección de datos deberá velar, a través de las funciones que le son encomendadas por el artículo 39 RGDP, por la integridad de principios del RGPD vistos en el capítulo 2.2.1. del Título III y sobre lo cual cabe añadir:

A) La licitud, la lealtad y la transparencia, con relación al interesado: el DPO deberá estar pendiente de los consentimientos y de que las excepciones se rijan por leyes que las regulen y del deber de secreto profesional. El principio de transparencia está muy relacionado con el deber información. Este deber de información está muy presente en el reglamento y con más motivo después de que la AEPD[601], exima de la obligación de solicitar consentimiento para la recogida y utilización de los datos personales, de tal forma que se entiende que el principio de transparencia debe prevalecer sobre el criterio de la AEPD y que el médico o el centro sanitario deberán informar al paciente de sus derechos en relación a sus datos.

B) La limitación de la finalidad: el DPO deberá tener en cuenta este principio al realizar los estudios de evaluación del impacto que deberá realizar el responsable del tratamiento de datos, ver capítulo 3.6 del Título II y valorar, en su caso, compatibilidades distintas de las que originan las recogidas de datos[602].

C) La minimización de datos: el DPO deberá tener en cuenta este principio al asesorar sobre los estudios de evaluación del impacto que deberá realizar el responsable del tratamiento de datos[603]. Aunque lo cierto es que los formularios de captación de datos en la sanidad pública vienen prestablecidos por la Administración Pública

[600] STC 37/2011 de 28 de marzo de 2011 (Sala Segunda), FD 5º.
[601] *Vid. Supra p 314,* capítulo 3.2.1., del Título III.
[602] *Vid. Supra p 232*, capítulo 4.1.5., del Título II.
[603] *Vid. Supra p 210,* capítulo 3.6., del Título II.

sanitaria y se sobreentiende que este principio esta respetado, por el principio de presunción de legalidad de los actos de la Administración Pública[604].

D) La exactitud de los datos: la propia naturaleza y finalidad de los datos relativos a la salud obliga al DPO a realizar auditorías para contrastar el nivel de adecuación y exactitud de los datos de las historias clínicas y tarjetas sanitarias de la organización sanitaria.

E) La confidencialidad: el DPO deberá tener en cuenta este principio al realizar los estudios de evaluación del impacto que deberá realizar el responsable del tratamiento de datos[605]. A su vez el DPO deberá realizar auditorías que indiquen el nivel de confidencialidad de los datos de las personas en todos los puntos de tratamiento de los mismos. Tal como se ha visto en el capítulo 3.6.5. del Título II, el DPO deberá diseñar o instar para que se diseñe un mapa de riesgos en puntos críticos en la confidencialidad de los datos previo análisis de riesgo y diseño de medidas de seguridad adecuadas a los riesgos[606].

F) Licitud de tratamiento: ya se ha tratado en el punto A).

G) El consentimiento: este principio requiere atención especial por parte del DPO, por los siguientes motivos. En primer lugar, es el único que se excepciona con la aplicación del artículo 9.2. del Reglamento 2016/679, pero este levantamiento o exención de este principio sufre excepciones, estas excepciones son las que la legislación de cada país impone a la limitación del consentimiento de la persona, es decir, una persona no puede decidir que sus datos se hagan públicos siempre y en todos los casos, sino solo en los que la ley no lo prohíbe o limita. En segundo lugar[607], la AEPD ha interpretado en una de sus publicaciones de 2019 que no es necesario que el médico o el centro sanitario solicite consentimiento para la recogida y tratamiento de los datos personales del usuario. Lo cual deberá reforzar la vigilancia del DPO en relación al deber de informar a la persona en relación a sus derechos, aunque no se le solicite su consentimiento. En tercer lugar, en base al artículo 9 del Reglamento (UE) 2016/679 se debe pedir consentimiento para tratar datos relativos a la salud de las personas según lo visto en el capítulo 3.2.3.3, capítulo 3.2.4.3. y capítulo 3.2.5.3 del Título III, salvo las excepciones del punto 2 del mismo artículo. El DPO este deberá revisar el EIPD[608] y deberá realizar auditorías[609].

[604] artículo 39.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas: los actos de las Administraciones Públicas sujetos al Derecho Administrativo se presumirán válidos y producirán efectos desde la fecha en que se dicten, salvo que en ellos se disponga otra cosa.

[605] *Vid. Supra p 210,* capítulo 3.6., del Título II.

[606] *Vid. Supra p 232,* capítulo 4.1.5., del Título II.

[607] *Vid. Supra p 318, capítulo* 3.2.1. del Título III.

[608] *Vid. Supra p 212.,* capítulo 3.6., del Título II.

[609] *Vid. Supra p 233,* capítulo 4.1.5., del Título II.

H) El consentimiento del menor: se aplica el mismo criterio que en el apartado anterior.

I) Las categorías especiales de datos: a esta categoría especial de datos personales se conocen como datos sensibles, se prevé para ellos una seguridad reforzada, frente a lo cual el DPO deberá realizar auditorías de adecuación e informar al responsable sobre la EIPD[610].

J) El tratamiento de los datos de naturaleza penal: no incumbe especialmente a los DPO de los centros asistenciales, ni debe actuar sobre ello.

K) El tratamiento de los datos sin identificación: no incumbe a los DPO de los centros asistenciales.

L) Otros principios: el Reglamento (UE) 2016/679 añade una serie de principios distintos de los mencionados con anterioridad de esta forma se refiere y que en relación a las funciones del DPO y en el sector sanitario, se refiere:

   a. al principio de periodos de conservación limitados; este principio se trata en el capítulo 3.2.3.1 del Título III. Este principio deberá ser tenido en cuenta por las evaluaciones del DPO dentro de cualquier centro sanitario.

   b. al principio de la calidad de los datos: en el sector de la salud este principio tiene una extremada importancia y está en conexión tanto con el principio de la protección de los datos desde el diseño como con el principio de la exactitud de los datos. Se entiende que deberá ser auditado por el DPO.

   c. al principio de la protección de los datos desde el diseño y por defecto: el DPO podrá evaluar este aspecto, sin embargo, por la naturaleza administrativa de los hospitales del sector público, salvo aquellos que tengan personalidad jurídica propia, se tendrá en cuenta que el diseño de datos ha sido creado por la Administración pública sanitaria y se le presume legalidad.

   d. al principio de las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes, artículo 47, Normas corporativas vinculantes, Reglamento (EU) 2016/679.

En resumen, en base al artículo 39 RGDP el delegado de protección de datos, tal como se ha descrito en el capítulo 4.1.5 del Capítulo II, tiene unas atribuciones y funciones determinadas. En relación a la protección de los principios del RGPD, en el sector sanitario público el DPO realizará asesoramiento general en todo lo relativo a los principios y obligaciones que impone el Reglamento (UE) 2016/679. El DPO deberá tener muy presente el principio más importante del RGPD, el principio de proactividad[611]. De tal forma deberá realizar supervisión y auditorías del cumplimiento de los principios del Reglamento (UE) 2016/679, de las políticas en materia de protección de esos principios,

[610] *Vid. Supra p 213,* capítulo 3.6., del Título II.
[611] *Vid. Supra p 95,* capítulo 3.1., del Título I.

así como de la concienciación y formación del personal implicados y obligados por la normativa. También deberá elaborar informes de evaluación de impacto sobre los principios de ciertos tratamientos de datos personales del artículo 35.b) del Reglamento (UE) 2016/679.

2.2. El delegado de protección de datos y la aplicación de los derechos en la protección de datos del RGPD que aparecen en el capítulo 2.2. del Título III

El capítulo 2.2 del Título III, sobre "Los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de los datos personales en el sector de la salud" hacen una descripción de los derechos de protección de datos cuando se refiere a datos relativos a la salud o a datos personales vinculados con organizaciones sanitarias. Por otra parte, el capítulo 4.1.5 del Título II describe las funciones del delegado de protección de datos y el capítulo 6 del Título III describe las funciones del delegado de protección de datos en el sector de la salud. El siguiente paso es abordar el rol del DPO en la aplicación de los derechos en la protección de datos del RGPD en el sector público.

Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario. En el capítulo 4.3 del Título II sobre "Intervención del delegado de protección de datos en caso de reclamación, Ley Orgánica 3/2018" se describe la nueva función del DPO en España. El derecho a presentar una reclamación está reconocido por el Reglamento (UE) 2016/679 en sus artículos 13, 14, 15, 47 y 77. La Ley Orgánica 3/2018 dedica el Título VIII a los procedimientos en caso de posible vulneración de la normativa de protección de datos, es decir, a la tramitación de una reclamación, dando al DPO un papel fundamental en la resolución de reclamaciones.

En el caso de los centros sanitarios ocurre lo mismo, la persona interesada puede dirigirse directamente al DPO para presentar una reclamación. Esta reclamación puede ir contra el responsable del tratamiento por incumplimiento del RGPD, antes de presentar la reclamación ante la Agencia Española de Protección de Datos o autoridad autonómica de protección de datos. El DPO dispondrá de un plazo máximo de dos meses para notificar su decisión.

La Autoridad de control también puede dirigirse al DPO para que conteste a una reclamación contra el responsable del tratamiento del centro en donde ejerza sus funciones. El DPO dispondrá de un plazo máximo de un mes para contestar.

De esta forma el PDO en cumplimiento de sus funciones, supervisará y auditará la efectividad de los derechos de las personas sobre sus datos en los centros sanitarios público y privados. En relación al capítulo 2.2 del Título III y el PDO en la sanidad pública cabe puntualizar:

1. Supervisará que el ejercicio del derecho al acceso a los datos de la persona interesada sea gratuito y ratificar la situación cuando el responsable entienda que son solicitudes "manifiestamente infundadas o excesivas especialmente debido a su carácter repetitivo".

2. Supervisará y auditará el ejercicio del derecho a la persona:
    a. a ser informada,
    b. a ser informada de la existencia y uso de decisiones automatizadas,
    c. a solicitar del responsable acceso a los datos,
    d. a retirar su consentimiento en cualquier momento, sin que ello afecta a la licitud del tratamiento basado en el consentimiento previo a su retirada,
    e. a presentar una reclamación frente al DPO y/o la Autoridad de control,
    f. a conocer ulteriores tratamientos a los que se someterán sus datos,
    g. al plazo de resolución de sus reclamaciones,
    h. a ejercer directamente o por medio de tu representante legal o voluntario.

El papel del DPO en relación a los derechos que proclaman el Capítulo III del Reglamento (UE) 2016/679 y el Título III de la Ley Orgánica 3/2018, en consonancia con el documento de la AEPD de diciembre de 2019 sobre "Guía para pacientes y usuarios de la sanidad", se desarrolla en estos términos:

A) La transparencia e información al afectado: el DPO supervisará y auditará los procedimientos de información al usuario o al paciente.

B) El derecho de acceso: el DPO supervisará y auditará los procedimientos de acceso del usuario o al paciente a los datos relativos a su salud o a sus datos personales en, es decir, al acceso a la historia clínica[612], a los datos que están en poder del responsable del tratamiento, de su tarjeta sanitaria[613] y a los datos de las recetas[614].

   El DPO también deberá supervisar que los profesionales sanitarios del centro o servicio que realice el diagnóstico o tratamiento del paciente o usuario tengan acceso a la historia clínica, entendiéndose también, con acceso a los datos de la tarjeta sanitaria y de las recetas prescritas, artículo 16.1 de la Ley 41/2002.

C) El derecho a la rectificación: el DPO supervisará y auditará los procedimientos de rectificación y actualización de los datos personales del usuario o paciente en poder del responsable del tratamiento de datos. A su vez, podrá supervisar la negativa, en su caso, de un profesional sanitario a la rectificación de los datos sanitarios de la persona.

D) El derecho a la supresión: el DPO supervisará y auditará, en el sector de la sanidad pública, los procedimientos del derecho supresión recogido en el RGPD y en la Ley Orgánica 3/2018[615], y modulado por el artículo 21 de la Ley 41/2002, y por el artículo 9.2.h) del Reglamento (UE) 2016/679.

[612] *Vid. Supra p 326*, capítulo 3.2.3.1., del Título III.
[613] *Vid. Supra p 357*, capítulo 3.2.5.1., del Título III.
[614] *Vid. Supra p 345*, capítulo 3.2.4.1., del Título III.
[615] Vid. Supra p 331, capítulo 3.2.3.1.; p 347, capítulo 3.2.4.1.; y p 359 capítulo 3.2.5.1.; del Título III.

E) El derecho a la limitación del tratamiento: igual que el punto anterior.

F) El derecho a la portabilidad: el DPO supervisará y auditará, en el sector de la sanidad pública, los procedimientos portabilidad[616]. Este derecho viene regulado por el artículo 18 de la Ley 41/2002.

G) El derecho de oposición: el DPO supervisará y auditará, en el sector de la sanidad pública, los procedimientos del derecho oposición recogido en el RGPD y en la Ley Orgánica 3/2018[617], y modulado por el artículo 21 de la Ley 41/2002, y por el artículo 9.2.h) del Reglamento (UE) 2016/679.

Con carácter general y en relación a los datos protegidos por el artículo 9 del Reglamento (UE), el DPO deberé supervisar y auditar la efectividad de los derechos que garantiza el RGPD y recordar al responsable del tratamiento será él quien deberá demostrar que han sido respetados.

Por último, el DPO en España tiene una función muy relevante en cuanto puede ser fuente de resolución de conflictos frente a reclamaciones contra el responsable del tratamiento de los datos[618], lo que en algunos casos determinadas entidades han venido a calificar como "El rol del DPO como mediador y de resolución extrajudicial de conflictos[619]".

[616] *Vid. Supra p 334,* capítulo 3.2.3.2., del Título III.
[617] Vid. Supra p 338, capítulo 3.2.3.3.; p 353, capítulo 3.2.4.3.; y p 365 capítulo 3.2.5.3.; del Título III.
[618] *Vid. Supra p 236,* capítulo 4.3, del Título II.
[619] Asociación Española para la calidad. Disponible en https://dpd.aec.es/el-rol-del-dpo-como-mediador-y-de-resolucion-extrajudicial-de-conflictos/. (31/05/2021)

Capítulo.3. El delegado de protección de datos y el tratamiento de los datos en el sector público de la salud

3.1. El delegado de protección de datos y el tratamiento de datos en el sector público de la salud que aparece en el capítulo 3 del Título III

En el capítulo anterior, la Tesis ha entrado a relacionar, por un aparte, los principios del RGPD y, por otra parte, la aplicación de los derechos en la protección de datos del RGPD, con el papel del delegado de protección de datos en el sector sanitario público.

De este análisis se concluye por una parte, que el DPO realizará asesoramiento general en todo lo relativo a los principios y obligaciones que impone el RGPD, así como realizará supervisión y auditoría del cumplimiento de los principios del Reglamento (UE) 2016/679, de las políticas en materia de protección de esos principios, así como de la concienciación y formación del personal implicados y obligados por la normativa y elaborará informes sobre la evaluación de impacto sobre los principios de ciertos tratamientos de datos personales del artículo 35.b) del Reglamento (UE) 2016/679. Por otra parte, el DPO deberé supervisar y auditar la efectividad de los derechos que garantiza el RGPD y en España puede ser fuente de resolución de reclamaciones contra el responsable del tratamiento de los datos.

Sin embargo, el DPO además tiene un rol especial en relación al propio tratamiento de los datos en el sector público da la sanidad. El sector público de la sanidad es Administración pública por lo que se regula por los principios que rigen en el funcionamiento de la Administración Pública, Ley 39/2015, de 1 de octubre, el Procedimiento Administrativo Común de las Administraciones Públicas.

En este orden de cosas, el tratamiento de los datos en el sector de la sanidad ha sido visto en el capítulo 3.2 del Título III y en base al artículo 34.1.i) de la Ley orgánica 3/2018 se entiende que en todos los centros en donde se realicen alguno de estos tratamientos de datos, básicamente la historia clínica, debe haber un delegado de protección de datos. La Ley Orgánica 3/2018 excluye de esta obligación a los consultorios médicos de práctica individual, si bien están sujetos al artículo 9 del Reglamento (U)E 2016/679.

Estudiado el capítulo 1.2.5.2 del Título III y el capítulo 3.2.4 del Título III, se entiende que los centros con tratamiento de recetas son subsidiarios de contar con un delegado de protección de datos, aunque no obligados por su tamaño. Si bien las recetas y su tratamiento se ajustan a lo indicado en el artículo 9 del Reglamento 2016/679, en el capítulo 6.1.2. del Título III se excluyen a las oficinas de farmacia por no alcanzar la escala mínima de la obligación de contar con los servicios de un delegado de protección de datos. Además, las oficinas de farmacia quedan excluidas de este capítulo por ser negocios privados dado que el capítulo se refiere a la sanidad pública.

Las tarjetas sanitarias han sido estudiadas en el capítulo 1.2.5.3 del Título III y en el capítulo 3.2.4 del Título III. El estudio del contenido de las tarjetas y del tratamiento de las mismas permiten afirmar que los centros en donde se almacenen los datos implicados en la tarjeta sanitaria y en los centros en donde se traten estos datos, deberá

haber un delegado de protección de datos. En base al artículo 37.3 del Reglamento (UE) 2016/679, los centros públicos de almacenamiento de tarjetas de datos o de tratamiento de los datos que contiene o facilita, podrán compartir un mismo DPO en base a su estructura y tamaño.

El tratamiento de datos para el RGPD, la Ley Orgánica 3/2018 y para el *sistema de protección de datos relativos a la salud* de la Disposición adicional decimoséptima de la Ley Orgánica 3/2018 es un complejo "conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales"[620], que en base a los estudiado en este capítulo 5.3 se compone de elementos básicos del tratamiento de datos, de elementos complementarios y de elementos adicionales en el tratamiento de datos.

En base a todo lo comentado, se entiende que el DPO deberá actuar supervisando y auditando y asesorando al responsable en el EPID sobre la adecuación a las normas de aplicación de este conjunto de operaciones.

3.2. El delegado de protección de datos y el tratamiento de datos en el sector público de la salud durante una alarma sanitaria

Esta Tesis ha abordado en su capítulo 3.5. del Título III el tratamiento de los datos personales relativos a la salud de las personas en la gestión de una pandemia, una vez que en el capítulo 5.6 del Título I se ha estudiado el tratamiento de datos personales en la gestión de una alarma sanitaria. Dos capítulos obligados en el contexto de esta Tesis por la aparición de la pandemia COVID-19 y el Estado de Alarma en España a través del Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, cuya situación se prorrogó con periodos intermedios de normalidad durante la primera mitad del año 2020. El tercer Estado de Alamar es aprobado por el Gobierno mediante el Real Decreto 926/2020, de 25 de octubre, por el que se declara el estado de alarma para contener la propagación de infecciones causadas por el SARS-CoV-2. Este tercer estado de alarma es prorrogado mediante el Real Decreto 956/2020, de 3 de noviembre, concretamente por su artículo 1. La duración de la prorroga establecida se extiende del día 9 noviembre de 2020 hasta el día 9 de mayo de 2021, ambos a las 00:00h.

Como se ha visto en el capítulo 5.6.4 del Título I que el Estado de Alarma, por motivos de salud pública, activa una serie de excepciones en el tratamiento de los datos de las personas con carácter general, sin embargo, siguen vigentes las garantías del RGPD que no sufren modificaciones.

El tratamiento de los datos relativos a la salud en el Estado de Alarma, por motivos de salud pública, se ha revisado en el capítulo 3.5.2 del capítulo III, viendo algunos de los casos prácticos que más han inquietado a la opinión pública.

Sin duda, todas estas excepciones solo afectan al principio del consentimiento para la legitimación del tratamiento de los datos personales, del artículo 6 del RGPD, y para el tratamiento de los datos del artículo 9.2 del RGPD. Estas excepciones no afectan al resto

[620] *Vid. Supra p 319,* capítulo 3.2.2., del Título III.

de principios vistos en el capítulo 3.1. del Título I y capítulo 2.1. del Título III, ni a los derechos descritos en el capítulo 4.1. del Título I y capítulo 2.2 del Título III.

El importante rol del PDO tratado en el capítulo 2.1 y capítulo 2.2 del Título IV se hace todavía más necesario a raíz de la situación excepcional que plantea el Estado de Alarma, por causa de salud pública, en relación a ciertos conflictos que han emergido, a raíz de las medidas de gestión de la pandemia, entre algunos derechos fundamentales entre sí y con algunos bienes jurídicamente protegidos, el derecho a la protección de datos, el derecho a la protección de la salud y el derecho a la libre movilidad dentro de la UE.

La gestión de la pandemia ha demostrado que se pueden poner en conflicto derechos fundamentales y bienes jurídicamente protegidos, lo cual hace más necesaria la figura del DPO con el fin de facilitar que el ciudadano y el profesional conozcan a quién consultar, con facilidad y eficacia, en caso de duda sobre las medidas que se van adoptando de los centros sanitarios y la imperiosa necesidad de facilitar que los poderes públicos respeten todo el contexto de los derechos fundamentales visto en el capítulo 2.3 del Título I sin tener que acudir a los tribunales, circunstancia que hacen penosas e ineficaces las garantías constitucionales.

Uno de los ejemplos de ello son casos que se analizan en el capítulo 5.6.5 del Título I, en concreto las recomendaciones de la Comisión Europea y los supuestos tratados en el capítulo 3.5 del Título III, del cual llama la atención el último de ellos, el supuesto del pasaporte o carnet de inmunidad del COIVD-19. Tras mucho debate, la Comisión Europea anunció en el mes de marzo de 2021 la elaboración de un reglamento[621] propuesta sobre un marco para la emisión, verificación y aceptación de certificados de interoperabilidad de vacunación, Certificado Verde Digital, básicamente para evitar los obstáculos a la movilidad que puede suponer que cada Estado miembro genere sus propios certificados sin contar con los certificados del resto de Estados miembros[622].

Por la gran confusión generada, la Comisión Europea emitió un comunicado en su página web el día 17 de marzo de 2021, el cual decía[623]:

> La vicepresidenta de Valores y Transparencia, Věra Jourová, ha declarado lo siguiente: El certificado digital verde ofrece una solución a escala de la UE para que los ciudadanos de la UE dispongan de una herramienta digital armonizada en apoyo de la libre circulación en la UE. Se trata de buen mensaje para la recuperación. Nuestro objetivo fundamental es ofrecer una herramienta fácil de utilizar, no discriminatoria y segura que respete

[621] EUR Lex. Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre un marco para la emisión, verificación y aceptación de certificados de interoperabilidad de vacunación, pruebas y recuperación a los nacionales de terceros países que residan legalmente o residan legalmente en los territorios de los Estados miembros durante el COVID -19 pandemia (Certificado Verde Digital) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021PC0140&qid =1617357403450&from=EN. (30/04/2021).

[622] Comisión Europea. Web oficial de la Unión europea. "Coronavirus: la Comisión propone un certificado digital verde" Disponible en https://ec.europa.eu/commission/presscorner /detail/es/ip_21_1181 (15/04/2021).

[623] Comisión Europea. Web oficial de la Unión europea. "Coronavirus: la Comisión propone un certificado digital verde" Disponible en https://ec.europa.eu/commission/presscorner /detail/es/ip_21_1181 (15/04/2021).

> plenamente la protección de datos. Además, seguimos trabajando en pro de la convergencia internacional con otros socios.

A lo cual el comunicado añade:

> El comisario de Justicia, Didier Reynders, ha declarado: "Mediante el certificado digital verde adoptamos un planteamiento europeo para que los ciudadanos de la UE y sus familiares puedan viajar con seguridad y con el mínimo de restricciones este verano. El certificado digital verde no será un requisito previo para ejercer el derecho a la libre circulación y no discriminará de ningún modo. Un planteamiento común de la UE no solo nos ayudará a restablecer gradualmente la libre circulación dentro de la UE y a evitar la fragmentación, también es una oportunidad para influir en las normas mundiales y dar ejemplo fundándonos en nuestros valores europeos, como la protección de datos".

Finalmente, la Comisión de la Unión Europea publica en su página web el día 20 de mayo de 2021 el "Certificado COVID Digital de la UE: el Parlamento Europeo y el Consejo alcanzan un acuerdo sobre la propuesta de la Comisión", a lo cual añade[624]:

> La Comisión acoge con satisfacción el acuerdo político provisional alcanzado hoy entre el Parlamento Europeo y el Consejo sobre el Reglamento que regulará el Certificado COVID Digital de la UE. Esto significa que el certificado (anteriormente denominado «certificado verde digital») podría estar listo a finales de junio, según lo previsto.
>
> Tras el acuerdo alcanzado por el Parlamento Europeo y el Consejo, el Certificado COVID Digital de la UE: abarcará la vacunación, los tests y la recuperación; estará disponible en formato digital y en papel, dependiendo de la elección de cada persona destinataria, e incluirá un código QR firmado electrónicamente; será gratuito, fácil de obtener y también podrán disponer de él las personas vacunadas antes de la entrada en vigor del Reglamento que lo regule; los Estados miembros también lo podrán utilizar con fines nacionales, en función de sus respectivas legislaciones; los Estados miembros se abstendrán de imponer restricciones adicionales de viaje a las personas titulares de un Certificado COVID Digital de la UE, a menos que dichas restricciones sean necesarias y proporcionadas para salvaguardar la salud pública; la Comisión también movilizará 100 millones de euros para proporcionar tests asequibles a los Estados miembros.
>
> El Parlamento Europeo y el Consejo deben adoptar ahora formalmente el acuerdo político. El Reglamento entrará en vigor el 1 de julio, con un período de introducción progresiva de seis semanas para la expedición de certificados en aquellos Estados miembros que necesiten más tiempo.

El Reglamento (UE) 2016/679 en sus Considerandos 77 y 97 presenta al delegado de protección de datos como una garantía de que se está aplicando correctamente el RGPD mediante su supervisión de las observancias internas del Reglamento (UE) por parte de responsables y encargados. Una situación especial de salud pública que legitima la activación de excepciones a los principios del Reglamento (UE) 2016/679, hace más evidente e importante la presencia del delegado de protección de datos en todos los ámbitos en donde la ley obliga su presencia y en especial en los centros que lleven a cabo tratamientos de datos relativos al artículo 9 del Reglamento (UE) 2016/679.

[624] Disponible en https://ec.europa.eu/commission/presscorner/detail/es/ip_21_2593 (31/05/2021)

TÍTULO IV. UNA PROPUESTA PARA LA CORRECTA APLICACIÓN DE LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO DE LA SANIDAD EN ESPAÑA

Capítulo.1. Un modelo de aplicación. El delegado de protección de datos en la sanidad pública de la Comunidad de Madrid, su coordinación y el manual de protección de datos

1.1. Primer paso. Descripción del escenario: la sanidad pública de la Comunidad de Madrid

El primer paso es la descripción del escenario, su definición, su naturaleza y la identificación de tratamientos de datos que lleva a cabo[625]. El siguiente paso es identificar la responsable y/o encargado del tratamiento de datos[626]. Por último, analizar la organización a estudio, básicamente su estructura, tamaño y volumen de operaciones. La Comunidad de Madrid organiza y estructura la sanidad pública entorno al Servicio Madrileño de Salud que tuvo su origen en el Servicio Regional de Salud creado por la Ley 9/1984, de 30 de mayo.

El artículo 58 de la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid, crea el Servicio Madrileño de Salud (Título VII), diciendo:

> 1. Se crea el Servicio Madrileño de Salud para llevar a cabo, en el ámbito de la Comunidad de Madrid, una adecuada configuración y asignación del presupuesto para la asistencia sanitaria de la población con derecho a cobertura asistencial en función de las necesidades estimadas y que permita, a su vez, una adecuada organización y ordenación del Sistema Sanitario de la Comunidad de Madrid.

Habitualmente los servicios sanitarios públicos y en ocasiones los privados, se organizan funcionalmente en base a lo que se viene a entender, por un parte, como el área de la Atención Especializada, que incluye todos los dispositivos en los cuales la atención sanitaria es provista por especialistas médicos, y por otra parte, el área de la Atención primaria, que incluye todos los dispositivos en los cuales la atención sanitaria es provista por médicos de familia y otros especialistas como, internistas, ginecólogos, pediatras y psicólogos, fuera de los hospitales. En algunos libros aparen otros niveles intermedios, cada vez más en desuso.

1.1.2. Red asistencial de Atención primaria

En base al Anexo II del Real Decreto 1030/2006, de 15 de septiembre, por el que se establece la Cartera de Servicios Comunes del Sistema Nacional de Salud y el procedimiento para su actualización, se entiende por atención primaria:

> La atención primaria es el nivel básico e inicial de atención, que garantiza la globalidad y continuidad de la atención a lo largo de toda la vida del paciente, actuando como gestor y

[625] *Vid. Supra p 314*, capítulo 3.2.1., del Título III.
[626] *Vid. Supra p 423,* capítulo 1., del Título IV.

> coordinador de casos y regulador de flujos. Comprenderá actividades de promoción de la salud, educación sanitaria, prevención de la enfermedad, asistencia sanitaria, mantenimiento y recuperación de la salud, así como la rehabilitación física y el trabajo social.

La Atención primaria en el Sistema Nacional de Salud comprende las modalidades de la atención sanitaria a demanda, programada y urgente tanto en la consulta como en el domicilio del enfermo; indicación o prescripción y realización, en su caso, de procedimientos diagnósticos y terapéuticos; actividades en materia de prevención, promoción de la salud, atención familiar y atención comunitaria; actividades de información y vigilancia en la protección de la salud; rehabilitación básica; atenciones y servicios específicos relativos a la mujer, la infancia, la adolescencia, los adultos, la tercera edad, los grupos de riesgo y los enfermos crónicos. La Atención primaria presta además, atención paliativa a enfermos terminales; atención a la salud mental en coordinación con los servicios de atención especializada; y algunos aspectos de la atención a la salud bucodental, a lo cual hay que añadir la prestación farmacéutica, tal disponen los Anexos II, IV y V del Real Decreto 1030/2006, de 15 de septiembre, por el que se establece la cartera de servicios comunes del Sistema Nacional de Salud y el procedimiento para su actualización.

En la Comunidad de Madrid, la Atención primaria programada y la urgente, se prestan en los Centros de salud (CS) y en los consultorios locales (CL), en más de 430 puntos físicos diferentes[627], mediante los servicios prestados por parte de 14.835 efectivos, a los cuales hay que añadir otros 2.136 efectivos del SUMA 112[628].

Tabla 8. Centros de Atención primaria de la Red del SERMAS (Fuente: Consejería de sanidad de la Comunidad de Madrid. Web corporativa a 31 de mayo de 2021) (elaboración propia)

Dirección asistencial		Centros de Salud	Consultorio Local	Suma
	Norte	34	71	105
	Este	38	11	49
	Sureste	40	20	60
	Sur	31	10	41
	Oeste	23	14	37
	Noroeste	41	25	66
	Centro	49		49
Total		256	151	407

En la Comunidad de Madrid la Atención primaria se organiza en torno a la gerencia de Atención primaria, la cual dispone de direcciones asistenciales para la gestión de los Centros de salud y consultorios. Se organiza en torno a siete direcciones asistenciales

[627] CONSEJERÍA DE SANIDAD. Madrid (2021) "La Gerencia de Atención primaria". www.comunidad.madrid/servicios/salud/atencion-primaria (31/05/2021).

[628] CONSEJERÍA DE SANIDAD. Madrid (2021) "Portal estadístico de personal del Servicio Madrileño de Salud". https://www.comunidad.madrid/servicios/ salud/portal-estadistico-personal-servicio-madrileno-salud (31/05/2021).

que coordinan los centros de su ámbito territorial: Dirección Asistencial norte, Dirección Asistencial este, Dirección Asistencial sureste, Dirección Asistencial sur, Dirección Asistencial oeste, Dirección Asistencial noroeste y Dirección Asistencial centro. Los centros se distribuyen según la Tabla 8[629] (Anexo [MM]).

1.1.3. Red asistencial de Atención especializada

En base al Anexo III del Real Decreto 1030/2006, de 15 de septiembre, por el que se establece la Cartera de Servicios Comunes del Sistema Nacional de Salud y el procedimiento para su actualización, se entiende por atención especializada

> La Atención especializada comprende las actividades asistenciales, diagnósticas, terapéuticas y de rehabilitación y cuidados, así como aquellas de promoción de la salud, educación sanitaria y prevención de la enfermedad, cuya naturaleza aconseja que se realicen en este nivel. La Atención especializada garantizará la continuidad de la atención integral al paciente, una vez superadas las posibilidades de la atención primaria y hasta que aquél pueda reintegrarse en dicho nivel.

La Atención especializada en el Sistema Nacional de Salud comprende la asistencia especializada, en consultas, asistencia especializada en hospital de día médico y quirúrgico, hospitalización en régimen de internamiento, apoyo a la atención primaria en el alta hospitalaria precoz y, en su caso, hospitalización a domicilio, indicación o prescripción, y la realización, en su caso, de procedimientos diagnósticos y terapéuticos, atención paliativa a enfermos terminales, atención a la salud mental, rehabilitación en pacientes con déficit funcional recuperable, a lo que se debe añadir la atención urgente, tal como se desprende de los Anexos III, y IV del Real Decreto 1030/2006, de 15 de septiembre, por el que se establece la cartera de servicios comunes del Sistema Nacional de Salud y el procedimiento para su actualización.

Tabla 9. Centros de Atención Especializad de red del SERMAS (Fuente: Consejería de sanidad de la Comunidad de Madrid. Web corporativa a 31 de mayo de 2021) (elaboración propia)

Red de servicios del SERMAS		SERMAS		PRIVADOS	Mº de Defensa	Suma
		COMUNIDAD AUTONOMA	SEGURIDAD SOCIAL			
	Públicos	20	11		1	32
	Privados			1		1
	Total	20	11	1	1	33

[629] CONSEJERÍA DE SANIDAD. Madrid (2021) "La Gerencia de Atención primaria". www.comunidad.madrid/ servicios/salud/atencion-primaria (31/05/2021).

El Servicio Madrileño de Salud dispone, dentro de lo que se entiende por Atención especializada, de una red de centros propios y de centros adscritos, entre todos suman 30 hospitales y 2 complejos hospitalarios, en total 36 centros hospitalarios[630].

Dentro de los centros propios, 30 hospitales y 2 complejos, se pueden diferenciar, los que la propiedad patrimonial recae en la Comunidad Autónoma, 19 hospitales y 1 complejo, de los que la propiedad es de la Seguridad Social, 10 hospitales y 1 complejo. En la red del SERMAS hay en centro privado, 1 hospital, y un centro del Ministerio de Defensa, 1 hospital. En la Comunidad de Madrid además hay dos centros de apoyo, la Unidad Central de Radiodiagnóstico y el Centro de Transfusión. Todos ellos suman 33 centros sanitarios con 14.358 camas, a fecha de 31/05/2021 ([Anexo NN]).

En cuanto a las oficinas de farmacia, en la Comunidad de Madrid hay 2.871 oficinas de farmacia autorizadas[631].

De acuerdo con los datos que constan en el Sistema de Información Poblacional de la Comunidad de Madrid (SIP-CIBELES) a fecha 31 de diciembre de 2019, la población titular de tarjeta sanitaria individual (TSI) emitida por la Consejería de Sanidad asciende a 6.859.181 personas[632], que incluye a los residentes en la Comunidad con derechos a la asistencia sanitaria pública más grupos de como personas desplazadas, procedentes de otras comunidades o países de la Unión Europea, o extranjeros sin autorización de residencia.

1.1.4. Red de investigación clínica y biomédica dependiente del SERMAS

El papel de la investigación en el campo sanitario ha sido reconocido y fundamentado como una de las actividades del sistema sanitario, así la Ley 14/1986, de 25 de abril, General de Sanidad, en el artículo 18.15 del capítulo II, de las actuaciones sanitarias del sistema de salud, del Título I, del Sistema de salud, en donde se reconoce como actividad propia del sistema sanitario "el fomento de la investigación científica en el campo específico de los problemas de salud, atendiendo a las diferencias entre mujeres y hombre", artículo 18.15 de la Ley 14/1986. El artículo 68 del Capítulo III, áreas de salud, del Título III, de la estructura del sistema sanitario público, de la Ley 14/1986, entiende que:

> Los centros hospitalarios desarrollarán, además de las tareas estrictamente asistenciales, funciones de promoción de salud, prevención de las enfermedades e investigación y docencia, de acuerdo con los programas de cada Área de Salud, con objeto de complementar sus actividades con las desarrolladas por la red de atención primaria.

[630] CONSEJERÍA DE SANIDAD. Madrid (2021) "Hospitales de la red del Servicio Madrileño de Salud". Disponible en https://www.comunidad.madrid/servicios/ salud/hospitales-red-servicio-madrileno-salud (31/05/2021).

[631] STATISTAS. Global No.1 Business Data Platform (28 agosto 2019) "Distribución del número total de farmacias de España en 2018, por comunidad autónoma". Disponible en https://es.statista.com/estadisticas/629225/numero-de-farmacias-por-comunidades-autonomas-en-espana/ (31/05/2020).

[632] CONSEJERÍA DE SANIDAD. Madrid (2019) "Memoria de 2019 del Servicio Madrileño de Salud". www.comunidad.madrid/servicios/salud/memorias-e-informes-servicio-madrileno-salud (31/05/2021).

El artículo 5 sobre el ámbito de la aplicación del objeto, artículo 1, de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, en su apartado d) se refiere concretamente a la investigación, artículo 5 de la Ley 16/2003. Además, la Ley 16/2003, dedica el capítulo IV plenamente a la investigación.

El artículo 2.3, sobre principios rectores, del Título I, disposiciones generales, de la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid, manifiesta que:

> "La protección de la salud, la ordenación y la organización del Sistema Sanitario de la Comunidad de Madrid, se ajustarán a los siguientes principios, en los términos previstos en la presente Ley" entre los principios de enumero de la letra a) a la o), en la letra b) entiende que "Concepción integral de nuestro Sistema Sanitario, incluyendo la promoción de la salud, la educación sanitaria, la prevención, la asistencia en caso de enfermedad, la rehabilitación, la investigación y la formación sanitaria", artículo 2 de la Ley 12/2001.

Así pues, concluyendo, la ley que ordena la sanidad pública de la Comunidad de Madrid incluye a la investigación sanitaria dentro del Sistema Sanitario en su concepción integral.

En cuanto a la investigación sanitaria la Consejería de Sanidad en su comunicación institucional a través de su página web declara que:

> Dentro del ámbito público sanitario, los principales agentes que desarrollan impulsan y llevan a cabo actividades de I+D+i (investigación, desarrollo científico-tecnológico y de innovación) son los Institutos de Investigación Sanitaria, los centros sanitarios, tanto de Atención primaria como de Atención Hospitalaria, las Fundaciones de Investigación Biomédica y las estructuras de investigación cooperativa.

Las Fundaciones de investigación Biomédica (FIB) del SERMAS son las responsables de gestionar la actividad investigadora que se desarrollan en la red de hospitales del Servicio Madrileño de Salud y de los Institutos de Investigación Sanitaria (IIS).

El SERMAS dispone de Institutos de Investigación Sanitaria (IIS) que son la asociación de universidades, centros de investigación, agrupaciones empresariales y/o centros tecnológicos en torno a un hospital docente universitario.

La Comunidad de Madrid dispone de 8 Institutos de Investigación Sanitaria acreditados, Real Decreto 279/2016, por el Ministerio de Economía y Competitividad a propuesta del Instituto de Salud Carlos III tras superar el proceso de evaluación que son en la actualidad[633]:

1. Instituto de Investigación Sanitaria San Carlos.
2. Instituto de Investigación Sanitaria Gregorio Marañón.
3. Instituto de Investigación Hospital 12 de Octubre.
4. Instituto de Investigación Hospital de La Princesa.

[633] MS. Ministerio de Sanidad (2021). "Institutos de Investigación sanitaria acreditados según comunidad autónoma". Disponible en https://www.mscbs.gob.es/estadEstudios/sanidadDatos/ tablas/ tabla29_2.htm (31/01/2021) .

5. Instituto de Investigación Sanitaria IdiPAZ.
6. Instituto de Investigación Sanitaria Puerta de Hierro.
7. Instituto Ramón y Cajal de Investigación Sanitaria.
8. Instituto de Investigación Sanitaria Fundación Jiménez Díaz.

Los Institutos de Investigación Sanitaria (IIS) no están considerados como personas jurídicas con personalidad propia y operan a través de la Fundación de Investigación Biomédica (FIB) asociada. Así pues, la FIB es su órgano de gestión y administración. El SERMAS cuenta con 8 Fundaciones de Investigación Biomédica, 7 en hospitales y una en Atención primaria, estas son:

1. FIB Clínico San Carlos.
2. FIB Doce de Octubre.
3. FIB Getafe.
4. FIB Gregorio Marañón.
5. FIB La Paz.
6. FIB La Princesa.
7. FIB Niño Jesús.
8. FIB Príncipe de Asturias.
9. FIB Puerta de Hierro.
10. FIB Ramón y Cajal.
11. FIB Atención primaria.

1.2. Segundo paso. El delegado de protección de datos en la sanidad pública de la Comunidad de Madrid, su coordinación y el Manual de Protección de Datos

1.2.1. Con carácter general

Una vez concluido el primer paso, estudiar el escenario, el siguiente paso no puede ser otro que detectar de qué manera y forma la estructura analizada previamente ha implantado la figura del delegado de protección de datos.

El Reglamento (UE) 2016/679 en su artículo 37.3 entiende que cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño, sin embargo, el artículo 34.1.l) de la Ley orgánica 3/2018 estipula que los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Es evidente que el Reglamento (UE) 2016/679 cuando, en su artículo 37.3, hace referencia al organismo público no incluye al organismo público de sanidad excluido

explícitamente por el artículo 34.1l) de la Ley Orgánica 3/2018 que actuando en el ámbito nacional, y sin restar objeto y ámbito a la ley, refuerza las exigencias de unos de sus preceptos.

En cualquier caso, en el supuesto de la existencia de base jurídica suficiente para la creación de un único delegado de protección de datos en la Administración de Sanidad Autonómica, este no podría estar ubicado en el nivel de administrativo de la Consejería de Sanidad o Salud, por razones obvias ya comentadas en la Tesis.

En el supuesto, meramente hipotético, de la existencia de un escenario jurídico habilitante para un solo DPO para todo, la ubicación del nivel de responsabilidad principal del tratamiento de datos de las personas relativos a la salud de los usuarios y pacientes del Sistema Sanitario público en los servicios centrales del Servicio Regional de Salud, dificultaría el cumplimiento de muchas de sus funciones relativas al responsable y ubicaría el nivel de responsable del tratamiento al más alto nivel dentro de la jerarquía de la administración Pública Sanitaria, circunstancia que, además de absurda, no se atiene a la consideración de responsable y encargado del tratamiento de datos del RGPD legalmente establecido.

Las Consejerías de Sanidad no pueden ni deben ostentar el papel de responsable ni encargado del tratamiento, pues, no atendiendo a la realidad, coloca artificialmente sobre el Consejero de Sanidad dicha responsabilidad, cuestión inabarcable. Por otra parte, la Administración sanitaria no debe alinear el concepto de dato tan solo al del registro informático pues en los centros sanitarios el soporte documental y las fuentes de datos[634] son mucho más extensas y amplias abarcando al soporte papel y el de las tarjetas sanitarias, entre otros. Los servicios centrales del Servicio Regional de Salud tampoco deben identificarse como responsable de los datos de los centros sanitarios de su ámbito de competencia por todo lo comentado con anterioridad.

En el supuesto estudiado, en la sanidad pública em España y en concreto en la Consejería de Sanidad de Comunidad de Madrid a 25 de mayo de 2021, habiendo entrado en vigor el RGPD el día 25 de mayo de 2018, todavía no hay delegados de protección de datos en los hospitales públicos ni en los hospitales públicos con personalidad jurídica propia y tampoco los hay en las unidades de coordinación o Dirección de Atención primaria, ni en el centro coordinador de la Base Poblacional de población protegida.

En base a la información que suministra la AEPD en su web se pueden conocer los centros que ya disponen a 25 de mayo de 2021 de delegado de protección de Datos y concretamente en el Servicio Madrileño de salud constan los siguientes DPOs[635]:

1. Fundación para la Investigación biomédica del Hospital Universitario la Paz.
2. Fundación para la Investigación biomédica del Hospital Universitario 12 de Octubre.

[634] *Vid. Infra p 427,* capítulo 1., del Título IV.

[635] AEPD (2021) "Consulta DPD" Disponible en https://sedeagpd.gob.es/ sede-electronica-web/ vistas/ infoSede/consultaDPD.jsf (30/04/2021).

3. Fundación para la Investigación biomédica del Hospital Universitario Clínico San Carlos.
4. Fundación para la Investigación biomédica del Hospital Universitario Gregorio Marañón.
5. Fundación para la Investigación biomédica del Hospital Universitario Puerta de Hierro Majadahonda.
6. Fundación para la Investigación biomédica del Hospital Universitario Hospital la Princesa.
7. Fundación para la Investigación biomédica del Hospital Universitario de Getafe.

1.2.2. Los delegados de protección de datos en los centros obligados del SERMAS

En el base al análisis del capítulo 1 del Título IV y de los capítulos 5 y 6 del Título III, y en virtud del artículo 34.1.I) de la Ley orgánica 3/2018 es evidente que se debe nombrar a un delegado de protección de datos en cada uno de los hospitales el Servicio Regional de Salud, así como un delegado de protección de datos de la Base de Datos de Población Protegida del Sistema Nacional de Salud y un delegado de protección de datos que englobe a un cierto número de Centros de salud y consultorios locales de Atención primaria, así como en las unidades de investigación biomédica del SERMAS.

La magnitud del Servicio Regional de Salud y el gran número de centros con responsables de tratamiento de datos obligará a nombrar a un número considerable de delegado de protección de datos, lo cual aconseja crear una Comisión Central de delegado de protección de datos en el SERMAS y también, la confección de un Manuela de Protección de datos para el SERMAS, con el objeto de unificar criterios y política de las medidas a aplicar.

En base al Reglamento (EU) 2016/679 y a la Ley Orgánica 3/208 el delegado de protección de datos, con dedicación parcial o total, puede ser contratado a tal fin, pudiendo recaer en una persona que esté ya en la plantilla del centro o puede recaer en una persona externa mediante contrato de prestación de servicios, en todo caso, el responsable debe estar en condiciones de poder dar su nombre y localización a todas las personas que acudan al centro o que lo soliciten, tal como dispone el RGPD en sus artículos 13, 14, 30, 33, 37 y 38.

A modo estimativo, exclusivamente, se entiende que debería haber un delegado de protección de datos en cada centro hospitalario o complejo, en total de 31. Además, se entiende que por el gran volumen de centros sanitarios que están bajo la Dirección de la gerencia de Atención primaria, cada Dirección Asistencial debería contar con un delegado de protección de datos, en total, 7 delegado de protección de datos en el área de Atención primaria. A lo cual debería sumarse un delegado de protección de datos para la unidad que gestiona la Base de Datos de Población Protegida del Sistema Nacional de Salud en la Comunidad Autónoma de Madrid. Se estima un total de 39 DPO.

Además el punto 2 de la Disposición adicional decimoséptima, de tratamientos de datos de salud, de la Ley Orgánica 3/2018, en su letra “h” ordena que el día 1 de diciembre de 2019 “los comités de ética de la investigación, en el ámbito de la salud, biomédico o del

medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679", añadiendo que esto deberá ocurrir cuando "comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados".

En este orden de cosas, los delegados de protección de datos de los hospitales actuaran en sus Comités de ética de la investigación, es decir, podrá ser el mismo dado que el responsable del tratamiento de datos es el mismo. Cuando estos hospitales dispongan de las Fundaciones de Investigación Biomédica, estas Fundaciones vinculadas al hospital deberán disponer de un delegado de protección de datos. Dado que el responsable del tratamiento de datos del hospital suele ser el mismo que el de la FIB y dado que los datos de la FIB son los del propio hospital, cabría plantearse que el delegado de protección de datos pudiera recaer en la misma persona, si bien parece que debería ser designado también por el responsable de la FIB. Es decir, dentro de la argumentación que se ha seguido sobre hospitales, comités de bioética y Fundaciones de Investigación de estos propios hospitales, se puede concluir que cada establecimiento deberá tener su delegado, aunque nada impide que pueda recaer sobre la misma persona física o jurídica.

Nade impide, sino incluso la lógica puede aconsejar, que la política de designación de delegados de protección de datos atendiendo a la cualificación que exige el artículo 35, cualificación del delegado de protección de datos, de la Ley Orgánica 3/2018, recaiga, en su caso, en personal que ya conste en la plantilla de los centro sanitario y/o asignando esta función a profesionales que la puedan compaginar con otras funciones compatibles, en aras de evitar en la mediad de lo posible la sobrecarga, si fuera innecesaria, del presupuesto público del SERMAS.

1.2.3. Comisión central de Delegados de Protección de Datos del SERMAS

En todo caso, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 no impiden que los Servicios Regionales de Salud creen unidades administrativas para la coordinación de los delegados de protección de Datos de los centros asistenciales, pero en ningún caso autorizan sustituir por otras figuras las creadas por el Reglamento (UE) 2016/679.

Una unidad de coordinación de los delegados de protección de datos en los Servicios Regionales de Salud debería depender directamente del máximo responsable del Organismo público y debería estar coordinada por un experto y dirigidos por una política única de protección de datos que podría, o mejor, debería estar reflejada en un Manual de Protección de Datos del Servicio Regional de Salud.

De tal forma, en la Comunidad de Madrid esta Comisión debería estar compuesta por los 39 DPO de la Consejería de Sanidad sea cual fuera su modalidad de contratación o designación.

Esta Comisión en su constitución y funcionamiento debería estar a lo dispuesto por el artículo 15 y siguientes de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, artículo 15 y ss. de la Ley 40/2015.

1.2.4. Manual de protección de datos del Servicio Madrileño de Salud

Como base previa a que los centros asistenciales realizaran su correspondiente evaluación del impacto relativa al tratamiento de datos[636], el SERMAS y en coordinación con la Comisión de delegados de protección de datos debería elaborar y editar un Manual de protección de datos cooperativo indicando la forma y manera de aplicar el Reglamento (EU) 2016/679 y la Ley Orgánica 3/2018 a todos los centros dependientes del SERMAS con criterios de unidad, equidad, eficacia e igualdad. En la elaboración de Manual el SERMAS se debería informar a la AEPD y contar con su asesoramiento y criterio.

Este Manual de protección de datos del Servicio Regional de Salud, podría ser el embrión de la confección de un código de conducta de protección de datos relativos a la Salud en la Comunidad Autónoma de Madrid, acordado entre la Administración pública sanitaria y las organizaciones de empresarios sanitarios del sector privado de la Comunidad Autónoma.

El Reglamento (UE) 2016/679 presenta una gran innovación en el terreno de las políticas de protección de datos de las personas, este es el principio de proactividad. Este principio actúa directamente sobre el responsable del tratamiento de tal forma que la Agencia Española de Protección de Datos en su Guía del Reglamento de Protección de Datos para responsables del tratamiento en su página explica el concepto de "principio de responsabilidad proactiva". Es decir, este principio es entendido por el Reglamento (UE) 2016/679 como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. Los códigos de conducta, artículo 40 del Reglamento (UE) 2016/679, aparecen como otro elemento de la proactividad[637]. La posibilidad de adherirse por parte de los responsable y encargados del tratamiento, artículo 40.3 del Reglamento (UE) 2016/679) a los códigos de conducta se entiende como una medida de seguridad, artículo 32.3 del Reglamento (UE) 2016/679.

El RGPD dota a los códigos de conducta máxima importancia, dando al Comité Europeo de Protección de datos las competencias para su impulso y aprobación[638].

1.3. Paso previo para el Código de conducta del sector de la Salud en la Comunidad de Madrid

1.3.1. Paso previo para el Código de Conducta del sector de la Salud en la Comunidad de Madrid

Con objeto de especificar la aplicación del presente Reglamento, tal y como aconseja el Reglamento (UE) 2016/679 con relación a los códigos de conducta, artículo 40.2 del

[636] *Vid. Infra p 210,* capítulo 3.6, del Título II.
[637] *Vid. Supra p 239,* capítulo 5.1., del Título II.
[638] *Vid. Supra p 184*, capítulo 1.2.1., del Título II.

Reglamento (UE) 2016/679, este código de conducta del sector de la salud en la Comunidad Autónoma de Madrid debería contemplar como mínimo:

a) el tratamiento leal y transparente
b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos
c) la recogida de datos personales
d) la seudonimización de datos personales
e) la información proporcionada al público y a los interesados
f) el ejercicio de los derechos de los interesados
g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño
h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32
i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;
j) la transferencia de datos personales a terceros países u organizaciones internacionales

A los que habría que añadir:

a. Criterios sobre el consentimiento informado en los centros asistenciales
b. Criterios sobre el consentimiento informado en el momento de la solicitud de la tarjeta sanitaria
c. Criterios sobre el consentimiento informado en el momento de la solicitud de la receta
d. Criterios sobre la información a suministrar al usuario y al paciente en relación al tratamiento de sus datos
e. Criterios sobre el maco para la aplicación del derecho al acceso, a la rectificación, a la supresión, limitaciones al tratamiento, la portabilidad y el derecho de oposición
f. Formatos para ejercer el derecho al acceso, a la rectificación, a la supresión, limitaciones al tratamiento, la portabilidad y el derecho de oposición
g. Formas y formatos para la información que aparecen en las pantallas de los monitores en los accesos a consultas externas, pruebas diagnósticas y urgencias.

Conclusiones

1. Conclusiones globales

RÉGIMEN BÁSICO DE LA PROTECCIÓN DE DATOS

Concepto jurídico de Dato

Dato puede ser cualquier representación simbólica. El dato es aquella realidad o hecho captado por el ser humano que una vez se junta con otra realidad o dato es capaz de aportar información o transmitir información sobre esa misma realidad. El término dato no debe confundirse con lo que coloquialmente es información, pues el dato es previo a la información.

Dato personal, es el que puede aportar información relativa a un individuo identificado o identificable, el resto es un dato anónimo. Al dato personal se le antepone a la expresión "dato de carácter personal", tras la STS 6188/1996. El dato de las personas es el hecho fáctico del derecho fundamental que se protege.

La confusión entre datos y datos informáticos, tal como si el control de los datos correspondiera tan solo a una función informática es muy frecuente. El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, es el que regula la seguridad de las redes y sistemas de información. También se debe distinguir entre gestión informática documental y gestión informática de bases de datos. Una trata al documento como un dato y la otra trata los datos internos del documento como datos.

Dato y documento están íntimamente ligados de tal forma que no hay documento sin datos. Documento es todo soporte material que exprese o incorpore datos, hechos o narraciones (artículo 26 del Código Penal). Los documentos electrónicos los regula el artículo 3 de la ley 59/2003 y la Ley 34/2002 acepta el valor probatorio en juicio del soporto electrónico.

El término fichero, aparece en el artículo 2.1 del Reglamento 2016/679 al describir su ámbito material, se entiende como conjunto ordenado de fichas y ficha como pedazos de papel o material donde se consignan datos. Sin embargo, el artículo 2.1 hace referencia a "datos personales contenidos o destinados a ser incluidos en un fichero", siendo fundamental el destino más que el soporte. En base al Considerado 15 del Reglamento 2016/679, "con el fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas" se debe entender fichero en los dos sentidos, en el tradicional y en el informático.

El anexo del ENI RD 4/2010, de 8 de enero, define el documento electrónico como: "información de cualquier naturaleza en forma

electrónica, archivada en un soporte electrónico según un formato determinado, y susceptible de identificación y tratamiento diferenciado."

Los dos textos legales, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 clasifican a los datos en dos grupos, uno, los afectados por esta normativa y otro, los no afectados. Dentro de los afectados, se encuentran, por una parte, los de categoría especial (artículo 9) y por otra parte, el resto de datos personales. Añade dentro de los datos protegidos los relativos a condenas penales (artículo 10), y los datos sin identificación (artículo11 del Reglamento 2016/679).

Los dos textos legales además, califican al dato cada vez que la norma se refiere a un caso concreto, de las distintas calificaciones, muchas de ellas funcionales, se desprenden treinta (30) formas distintas de entender el dato, así contempla el dato: anonimizado, biométrico, bloqueado, de carácter personal, censal, clínico-asistencial, concreto, de contacto, exactos, facilitados, con fines de interés público, genéticos, de identificación, de identificación del paciente, procedentes de imágenes y sonidos, imprescindible, incompleto, inexacto, localización, de menores de edad, necesarios, de documentos, personales, rectificados, de salud, de investigación, seudonimizado, de tráfico, tributario, y de vida sexual.

El concepto de dato no está definido en ninguno de los textos vigentes relativos a la protección de datos. Lo que sí está definido es el concepto de dato personal, concretamente lo define el Reglamento (UE). A efectos del Reglamento (UE) es el dato no anónimo, es el dato que permite identificar a una persona determinada. Es un identificador.

En este contexto, para el Reglamento (UE) 2017/679, el dato es información, pues el dato o los datos que no generan información no son susceptibles de aplicarse a esta norma.

La normativa europea, tanto la derivada como la nacional, relativa a la protección de datos protege el dato de las personas física y más concretamente el dato y el derecho fundamental de la persona física de controlar el tratamiento de estos datos.

El ámbito de aplicación del Reglamento 2016/679, de protección de datos, el control del tratamiento que se haga de los datos para proteger los derechos fundamentales de las personas nada tienen que ver con el soporte del dato, pues lo que se controla es solo su tratamiento, la característica del soporte sobre el que esté el dato (papel, digital, u otro) es una consideración menor.

El derecho fundamental de la protección de datos

La doctrina los define como un derecho declarado por una Constitución que goza de máximo nivel de protección. Un derecho en un texto constitucional se convierte en derecho fundamental, básicamente su regulación se exige por reserva de ley orgánica y respeto a su contenido esencial. Estos derechos constan en el Título I de la Constitución española, "De los derechos y deberes fundamentales", y se pueden clasificar en tres tipos: 1. Derechos fundamentales y libertades públicas, artículos 14 a 29; 2. derechos fundamentales básicos (Derechos y deberes de los ciudadanos), artículo 30 a 38; 3. Derecho fundamentales informadores (Principios rectores de la política social y económica), artículo 39 a 52.

Conforme a los artículos 9 y 53 CE, todos los poderes públicos, incluidas las diferentes Administraciones Públicas, se encuentran vinculados por los derechos fundamentales.

Los derechos fundamentales en el marco de nuestro Estado constitucional de derecho deben ser analizados teniendo en cuenta tres claves: no hay derechos fundaméntales absolutos, la igualdad de valor y rango de todos los derechos fundamentales exige llevar a cabo en cada caso de conflictivo una ponderación y las limitaciones de derechos fundamentales tienen que ser establecidas por normas con rango de Ley orgánica que han de respetar el contenido esencial de aquellos.

El derecho a la protección de datos es un derecho fundamental en base al Considerando 1 del Reglamento 2016/679, al artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea y en especialmente en base al artículo 18 de la Constitución Española y a la STC 94/1988, entre otras sentencias.

La resolución de conflictos entre derechos fundamentales entre sí o con bienes jurídicamente protegidos se debe afrontar desde dos planos distintos: el plano normativo o ámbito de regulación y el plano en la aplicación del Derecho (de las normas vigentes). Dentro del plano de regulación destaca las garantías de la reserva de ley orgánica, la jerarquía normativa y el respeto al contenido esencial. Dentro del plano de aplicación del derecho cabe destacar la teoría de la ponderación y la de proporcionalidad ("test de la proporcionalidad" o "test alemán de proporcionalidad").

Se puede afirmar que la regulación del derecho fundamental a la protección de datos de carácter personal ha tenido un impacto singular en las técnicas e instituciones clásicas del Derecho Administrativo.

Los principios de la protección y del tratamiento de datos en la normativa de protección de datos personales	El primer principio, es el principio de proactividad o principio de la responsabilidad activa, es decir, no basta con hacerlo bien, sino que se debe poder demostrar. El segundo principio del Reglamento 2016/679), es el principio de la protección pasiva de todos los datos personales, ubicando la carga de la prueba en quien realiza el tratamiento del dato y no en su titular. El tercer principio, es el de la minimización del tratamiento de datos. Los principios que operan en el RGPD y en la Ley Orgánica, son: La licitud, la Lealtad y la transparencia, la limitación de la finalidad, la minimización de los datos, la exactitud de los datos, la confidencialidad, la licitud de tratamiento, el consentimiento, el consentimiento del menor, las categorías especiales de datos, el tratamiento de los datos de naturaleza penal y el tratamiento de los datos sin identificación. Otros principios: periodos de conservación limitados, calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento y los requisitos para las transferencias internacionales.
Los derechos que hacen posible la efectividad de la aplicación del derecho a la protección de los datos personales	El Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, son normas que proclaman y defienden el derecho a la protección de las personas, la protección de su intimidad. El primer derecho que protege es la protección de las personas físicas en lo que se refiere a los datos personales. El segundo derecho que protege son los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. Por último, el Reglamento (UE) defiende el derecho a la libre circulación, tan solo que atendiendo a una serie de cautelas y reglas que el propio Reglamento (UE) específica y desarrolla. Además, protege: la transparencia e información al afectado, el derecho de acceso, el derecho a la rectificación, el derecho a la supresión, el derecho a la limitación del tratamiento, el derecho a la portabilidad y el derecho de oposición. Otros derechos, Reglamento (UE) 2016/679: derecho a presentar una reclamación ante una autoridad de control; el derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento; representación de los interesados, y derecho a indemnización y responsabilidad.
Tratamiento de los datos en base a la	El tratamiento solo está permitido cuando esto este sea lícito en función de la base jurídica del artículo 6.1 y no estén prohibidos por el artículo 9. El tratamiento de datos personales está autorizado solo

norma de protección	cuando se cumple una de las bases jurídica de las seis condiciones del artículo 6 del Reglamento y cuando el dato está sujeto al artículo 9 deberá cumplir una de las diez condiciones del artículo 9.2 y la del artículo 9.3. En cuanto al acto de consentimiento, no vale cualquier acto sino aquel que reúne las condiciones del artículo 7 del Reglamento y en especial las del artículo 8, en los menores de edad. Así mismo, el consentimiento no tiene un valor absoluto, artículo 9 del Reglamento (EU). El artículo 4 del RGPD es el que define la expresión tratamiento de datos, a efecto del ordenamiento jurídico. Es, pues, cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. El Tratamiento de datos tiene a criterio de esta Tesis tres categorías: elementos básicos del tratamiento de datos (los que aparecen en el artículo 4 del RGPD), elementos complementarios del tratamiento de datos (los que no aparecen en el artículo 4 del RGPD pero aparecen en el RGPD) y elementos adicionales del tratamiento de datos (los que no son ni básicos ni complementarios). En este orden de cosas, los elementos básicos del tratamiento de datos son: “todas las operaciones directas sobre datos que se pueden producir sobre los datos personales y que requieren de protección por parte del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 y que aparecen en el artículo 4, definiciones, del Reglamento (UE) 2016/679.” Contemplan las siguientes operaciones: acceso; adaptación y modificación; conservación; comunicación y difusión; cotejo; destrucción; extracción, consulta y utilización; interconexión; limitación; organización y estructuración; recogida y registro de datos; y supresión. Los elementos complementarios del tratamiento de datos, son: todas las operaciones o acciones sobre datos que no están incluidas en el artículo 4, definiciones, del Reglamento (UE) 2016/679, en el punto relativo a tratamiento, pero que o son acciones u operaciones previas al tratamiento de los datos personales o son colaterales al tratamiento de datos o que son necesarias para que este tratamiento sea lícito. Contemplan las siguientes acciones: anonimización y seudonimización; bloqueo; circulación y portabilidad; mantenimiento; minimización; exactitud de datos; rectificación;

reidentificación; reutilización; tráfico; y transferencia y transmisión internacional.

Los elementos adicionales en el tratamiento de datos personales, son: las acciones u operaciones adicionales que se pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley Orgánica 3/2018 o en alguno de ellos. Contemplan las siguientes acciones: automatización; confidencialidad y consentimiento; y oposición.

La licitud del tratamiento de las categorías especiales de datos se consigue a través de una de estas 6 vías: 1.por consentimiento; 2.por exigencia legal, por contrato o por ley; 3.por intereses vitales de cualquier persona física; 4.por interés público; 5. por ejercicio de la autoridad pública y 6. Interés legítimo del responsable del tratamiento.

El artículo 9, a su vez, excluye de la prohibición determinadas circunstancias, es decir, siguen siendo datos de categoría especial pero que una circunstancia ajena permite su tratamiento. La exclusión afecta tan solo al principio del consentimiento, no afectando al resto de principios.

Las exclusiones de la prohibición del artículo 9 lo son: 1. Circunstancias que afectan a la persona física, afectado o tercero: a.cuando el interesado haya hecho públicos sus datos personales; b.cuando haya consentimiento; y c.cuando es necesario para fines de salud; 2. Circunstancias ajenas a la persona afectada: a. atribuidas por funciones de potestad; b. afectadas por el interés general; y c. otras. Si bien el interés público esencial del artículo 9.2.g se entiende que debe ser un interés general reforzado en base a la STC de 2019 y a la STJUE de 2014.

Las bases jurídicas que legitiman a las personas, en el RGPD, para el tratamiento lícito de los datos del artículo 9 son: los profesionales sujetos a la obligación de secreto profesional, o bajo su responsabilidad y cualquier otra persona sujeta también a la obligación de secreto. En la Tesis aparece como “secreto profesional sobrevenido”.

La situación creada por la epidemia-pandemia del SARS-Cov-2 en el mes de marzo de 2020 en España, durante la elaboración de esta Tesis doctoral, obliga dedicar un espacio a las consecuencias de esta situación especial en el tratamiento de datos personales.

El ordenamiento jurídico español, en su ámbito estatal, hace referencia a la salud pública básicamente en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública;

en la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud; y en la Ley 33/2011, de 4 de octubre, General de Salud Pública. En cuanto al ámbito autonómico, la salud pública esta transferida a las Comunidades Autónomas.

La Ley 33/2011 en su capítulo I (la vigilancia en salud pública) dentro de su Título II (Actuaciones en salud pública), dedica el artículo 12 a la vigilancia en salud pública diciendo, a tenor literal: "La vigilancia en salud pública es el conjunto de actividades destinadas a recoger, analizar, interpretar y difundir información relacionada con el estado de la salud de la población y los factores que la condicionan, con el objeto de fundamentar las actuaciones de salud pública"

A su vez, el artículo 13, sobre la articulación de la vigilancia en salud pública, crea una articulación diluida y poco eficaz, así lo expresa la Ley: "1. Corresponde a la Administración General del Estado, a las comunidades autónomas, a las ciudades de Ceuta y Melilla y a la Administración local, en el ámbito de sus competencias, la organización y gestión de la vigilancia en salud pública."

El artículo 14 de la Ley 33/2011 encomienda la Ministerio de Sanidad la gestión de alertas de carácter supraautonómico o que puedan trascender del territorio de una comunidad autónoma y de alertas que procedan de la Unión Europea, la Organización Mundial de la Salud y demás organismos internacionales y, especialmente, de aquellas alertas contempladas en el Reglamento Sanitario Internacional, en su caso, en coordinación con las comunidades autónomas y las ciudades de Ceuta y Melilla. Las Actuaciones coordinadas en salud pública y en seguridad alimentaria del artículo 65 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, así como la coordinación y evaluación de la Red de Vigilancia en salud pública.

España tiene legislación especial en salud pública, la Ley 33/2011, de 4 de octubre, General de Salud Pública. Esta norma tan solo hace una referencia a las epidemias en su Disposición adicional cuarta. El término pandemia aparece en el capítulo artículo 33 (La actuación sanitaria en el ámbito de la salud laboral).

La Ley 33/2011 encomienda a los poderes públicos la función de la vigilancia en salud pública en el Capítulo I, mediante el artículo 12 (De la vigilancia en salud pública), el artículo 13 (Articulación de la vigilancia en salud pública) y el artículo 14 (De las competencias en Vigilancia en salud pública del Ministerio de Sanidad, Política Social e Igualdad).

En una epidemia los casos afectados se tratan a nivel clínico con los mismos datos que en cualquier otro supuesto. Los estudios y el

seguimiento de una epidemia o de una pandemia son estudios de carácter poblacional. Los datos que se utilizan en la epidemiología, una de las ciencias que sustenta la disciplina de la salud pública, suelen ser datos personales, pero no identificables, es decir, si bien son datos relacionados con la salud de las personas, no son datos identificables. En estas circunstancias no se deben aplicar las normas de protección de datos vigentes.

La Ley Orgánica 4/1981, de 1 de junio de Estados de Alarma, Excepción y Sitio, es la que regula el Estado de Alarma. En este orden de cosas, el Gobierno aprobó el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, en base al cual el Ministerio de Sanidad emitió la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19. Es muy difícil de defender que el rango de esta norma sea suficiente para los fines a los cuales está destinada, es decir, regular derechos fundamentales, como es la protección de datos de carácter personal, sobre el que la Constitución Española (artículo 53 CE) establece una reserva de ley.

Las situaciones de excepción que aparecen en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018 se comportan como supuestos de activación, la crisis en salud pública, en consecuencia, se deben incluir las alertas sanitarias producidas por una epidemia o pandemia. El Considerando 45 del Reglamento (UE) 2016/679 entiende que la exclusión de la prohibición es posible si hay normas de aplicación, de rango suficiente, que regulen lo excepcionado. Además, las situaciones de excepción solo afectan al consentimiento de las personas y mantiene las garantías los principios de licitud, lealtad y transparencia, el de la limitación de la finalidad y el de minimización de datos.

El Boletín Oficial de la Unión Europa publica el día 17 de abril de 2020 el documento “La Comisión Europea Comunicación 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 2020/C 124 I/01”.

INSTITUCIONES DE CONTROL, REGULACIÓN, TRATAMIENTO, COOPERACIÓN Y AUTORREGULACIÓN EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Los órganos de control

La Comisión Europea supervisa la aplicación del Derecho de la Unión Europea, el respeto a los Tratados de la Unión por parte de los Estados miembros, el cumplimiento de los Reglamentos y además preside los comités para la aplicación del Derecho de la Unión.

La Comisión, en el Reglamento (UE) 2016/679, tiene role en las cláusulas tipo, mecanismos de cooperación internacional, para disponer del Informe Anual de actividades emitido por cada Autoridad de control, para disponer del Informe anual del Comité y para adoptar actos de ejecución en código de conducta, mecanismos de certificación y los sellos y marcas de protección de datos, decisión de adecuación, asistencia mutua y las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité.

El Comité Europeo de Protección de Datos (CEPD) es un organismo europeo independiente para la aplicación coherente de las normas de protección de datos en toda la UE promoviendo la cooperación entre las autoridades de control de la UE. Se rige por los principios: la independencia e imparcialidad; la buena gobernanza, integridad y buena conducta administrativa; la responsabilidad colegial; la cooperación; la transparencia; la eficiencia y modernización; y la proactividad. Su funciones son: supervisar y garantizar la correcta aplicación del presente Reglamento, asesorar a la Comisión, emitir directrices, recomendaciones y buenas prácticas, examinar, alentar la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad, realizar la acreditación de los organismos de certificación, promover la cooperación y llevar un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

El Supervisor Europeo de Protección de Datos es la Autoridad de control independiente que supervisa la aplicación de las disposiciones del Reglamento (UE) 41/2001 a todas las operaciones de tratamiento realizadas por las instituciones y organismos comunitarios y velará por los derechos y libertades fundamentales de las personas físicas, en particular el derecho de las mismas a la intimidad, para que sean respetados por las instituciones y los organismos comunitarios, por lo que respecta al tratamiento de los datos personales, artículo 41, Reglamento (CE) No 45/2001.

Autoridad de control en los Estados miembros	A efectos del Reglamento (UE) la Autoridad de control es la/s entidad/es, designadas por cada Estado Miembro de la UE, en los propios Estados, encargada/s de la supervisión de la aplicación y cumplimiento del Reglamento y coherencia en la UE, cooperando entre sí y con el Comité Europeo de Protección de Datos, artículo 51.1 y 51.2 del Reglamento (UE) 2016/679. El artículo 54 del Reglamento (UE) 2016/679, exige a los Estados Miembros que la regulación de su Autoridad de control se realice por medio de una ley. Las potestades de la Autoridad de control que asigna el Reglamento (UE) 2016/679 son la correctiva y sancionadora, la de autorización y consultivos y la de investigación. En España la Autoridad de control viene regulada en el Titulo VII (Autoridades de Protección de Datos) del artículo 44 a 62 de la Ley Orgánica 3/2018. Se regula la Agencia Española de Protección de Datos, artículo 44 a 56, y de los artículos 57 a 62. También regula a la AEPD el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y por descontado por el Reglamento (UE) 2016/679. La Agencia Española de Protección de Datos desarrolla su actividad de investigación a través de las actuaciones previstas en el Título VIII (Procedimientos en caso de posible vulneración de la normativa de protección de datos) y de los planes de auditoría preventivas, artículo 51 de la Ley Orgánica 3/2018. La Autoridad Nacional de Seguridad para la Protección de la Información Clasificada, en la excepción en cuanto a las funciones de la AEPD.
Responsable del tratamiento y encargado del tratamiento	Las figuras del responsable del tratamiento y la del encargado del tratamiento son de extremada importancia tanto en el Reglamento (UE) 2016/679 como en la Ley 3/2018, sobre ellos recae toda la responsabilidad del tratamiento de datos y además la designación del delegado de protección de datos, artículo 37 del Reglamento (UE) 2016/679 y artículo 34 de la Ley 3 /2018. Se puede afirmar que salvo la figura de la autoridad de protección de datos (nacional y autonómica) y la figura del Comité Europeo de Protección de Datos, todo el desarrollo del Reglamento (UE) 2016/679 recae sobre las figuras del responsable y del encargado del tratamiento. Según la Comisión Europea, el responsable del tratamiento es el que utiliza y maneja los datos o quien decide cómo se manejan (tratan) y en base a qué criterio o fin. Los encargados del tratamiento manejan

o trata los datos como encargo o mandato del responsable del tratamiento.

La relación entre el responsable y el encargado del tratamiento es directa y nace única y exclusivamente de un acto jurídico, a ser posible de un contrato y mejor si es escrito, Artículo 28.1 del Reglamento (UE) 2016/679.

El responsable del tratamiento de los datos y en su caso el encargado que haya contratado deberá llevar un registro, anotación o agenda de las actividades que realicen, sustituyendo a la inscripción de ficheros de la anterior LOPD 15/1999 no vigente.

El responsable del tratamiento deberá vigilar la Protección de datos desde el diseño y por defecto del artículo 25 del Reglamento (UE) 2016/679. El responsable del tratamiento garantizará que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

La AEPD en septiembre de 2019, editó el modelo de Cláusula para contratos de encargados de tratamiento.

En este orden de cosas, la AEPD establece el criterio de "obligación de resultado" exigible por la jurisprudencia en relación a la obligación de establecer medidas de seguridad suficientes para impedir el acceso de datos de terceros.

A su vez, la AEPD entiende que, para garantizar este nivel de seguridad exigible en las tres vertientes de la seguridad, son necesarias medidas técnicas como organizativas.

El artículo 32 (Seguridad del tratamiento) dentro la sección 2 (Seguridad de Datos) del capítulo IV (responsable del tratamiento y encargado del tratamiento) del Reglamento (UE) 2016/679 entiende que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Cuando se produce una violación de la seguridad de los datos personales se deberá notificar, el responsable o el encargado, a la Autoridad de control sin demora y a más tardar 72 horas después de que hayan tenido constancia de ello.

La notificación a la Autoridad de control le corresponde al responsable del tratamiento, en el supuesto de que hubiera un encargado del tratamiento, este deberá notificar la violación de la seguridad de los datos al responsable del tratamiento.

La Evaluación de Impacto en la Protección de Datos Personales (EIPD) es una herramienta, con carácter preventivo, que debe aplicar el

responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. Regulada en el Reglamento (UE) 2016/679 por el artículo 35, de la Sección 3 (La Evaluación de Impacto en la Protección de Datos Personales). Será necesaria cuando un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, artículo 35.1, cuando lo determine la Autoridad de control, artículo 35.4 y en tratamientos automatizados, como la elaboración de perfiles y que produzcan efectos jurídicos para las personas físicas, artículo 35.3.a). También será precisa la EIPD en tratamientos a gran escala de las categorías especiales de datos del artículo 9.1 o de los datos personales relativos a condenas e infracciones penales del artículo 10, artículo 35.3.b), y en observaciones sistemáticas a gran escala de una zona de acceso público, artículo 35.3.c).

La diferencia principal entre la EIPD y los análisis de riesgos tradicionales reside en que la EIPD se realiza desde "el punto de vista del interés del sujeto" mientras que los análisis de riesgos se realizan desde el punto de vista del "riesgo para la entidad". El análisis de riesgo es la segunda fase de evaluación de impacto relativa a la protección de datos del Reglamento (UE) 2016/679.

La Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos de la AEPD es el documento de la Autoridad de control independiente del Estado Español de referencia para todos los responsables de tratamiento de datos.

La elaboración del plan de acción constituye la cuarta fase del proceso de la evaluación del impacto en protección de datos personales.

La identificación de riesgos permite la construcción de mapas de riesgos: son métodos de prevención que detectan los riesgos y amenazas para la actividad humana. Un mapa de riesgos es una herramienta, basada en los distintos sistemas de información, que pretende identificar las actividades o procesos sujetos a riesgo, cuantificar la probabilidad de estos eventos y medir el daño potencial asociado a su ocurrencia.

La consulta previa del Reglamento (UE) 2016/679. La consulta previa es una herramienta de consulta (obligada) cuando el EIPD demuestra que el tratamiento puede entrañar riesgos no asumibles para las personas. La consulta previa obliga a actuar a la Autoridad de control en relación al artículo 58 del Reglamento (UE) 2016/679.

Delegado de protección de datos (DPO)

Los elementos clave de la nueva legislación, después del principio de proactividad y del principio de protección pasiva, son, por una parte, el reforzamiento del consentimiento del interesado y, por otra parte, la creación de la figura del DPO.

La figura operativa más relevante es la del DPO, designado bien por el responsable o bien por el encargado de protección de datos.

Los aspectos relevantes y característicos de esta figura, son: independencia, designación, revocación, requisitos para ser designado, modalidades de contratación, funciones, obligaciones y régimen de responsabilidad y, por último, la relación que tiene con el responsable del tratamiento de datos y con el encargado del tratamiento de datos, en su caso.

Una de las características que definen al DPO es su independencia en relación a la personas o personas que le nombran, designan o contratan, artículo 38 (Posición del delegado de protección de datos) del Reglamento (UE) 2016/679. La Ley Orgánica 3/2018 es más explícita que el Reglamento en cuanto a la independencia del delegado de la protección de datos, pues el artículo 36 (Posición del delegado de protección de datos), apartado 2, dice: "Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses".

La designación tendrá carácter obligatorio, artículo 37.1 del Reglamento (UE) 2016/679, siempre que el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial. La Ley Orgánica 3/2018 en su artículo 34.1 (Designación de un delegado de protección de datos) amplia la lista de situaciones en las que se debe designar, el responsable o el encargado, a un DPO. Los responsables o encargados del tratamiento también podrán designar de manera voluntaria un DPO.

El DPO será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones del artículo 39 y artículo 37.5 del Reglamento (UE) 2016/679). La ley amplia las exigencias del requisito de idoneidad del DPO introduciendo el mérito de los certificados de capacitación voluntarios, artículo 35. En el plazo de diez días se comunicará a la Autoridad de control competente.

Los requisitos de la Ley Orgánica 3/2018 sobre los que ya expone el Reglamento (UE) 2016/679, son: demostrar que cumple los requisitos, serán valorados los mecanismos de certificación de los requisitos que presenta el candidato como mecanismo voluntario

para la demostración de los mismos, titulación universitaria que acredite conocimientos especializados en el derecho y práctica en materia de protección de datos.

Las formas o modalidades del DPO son bien el contrato laboral, se entiende en cualquier de sus modalidades, o bien el contrato de prestación de servicios profesionales de los artículos 1.252 al 1.314 del Código Civil.

Las funciones del delegado de protección de datos serán de información, asesoramiento, supervisión e intermediación extrajudicial y se encuentran especificadas en el artículo 39 del RGPD y en el artículo 34 y ss, y artículos 37 y 65.4 de la Ley Orgánica 3/2018, así como en el documento "directrices de los delegados de protección de datos de la AEPD".

El DPO tendrá las funciones de supervisar y gestionar. Por una parte, supervisará el cumplimiento de la normativa de protección de datos personales y, por la otra parte, cuando así se lo requiera el interesado gestionará las consultas en relación con el tratamiento de sus datos personales. Además, la Ley Orgánica 3/2018 incorpora en España una nueva función al delegado de protección de datos, esta nueva función viene estipulada en el artículo 37 sobre la "Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos. A lo que hay que añadir el artículo 65.4 de la Ley Orgánica /2018.

Por otra parte, del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 se concluye que el delegado de protección de datos debe desempeñar sus funciones dentro de las dependencias del centro responsable, es decir, en sus instalaciones.

La autorregulación en la protección de datos

Un Código de conducta es documento sobre principios, suscrito voluntariamente por una organización y que se compromete a cumplir unilateralmente.

Podrán ser elaborados por asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento, o modificar o ampliar dichos códigos. La adhesión a un código de conducta permitirá al responsable y al encargado del tratamiento poder demostrar la existencia de medios suficientes. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente. Los proyectos de código serán sometidos al mecanismo de coherencia a través de la Agencia

Española de Protección de Datos o, en su caso, las autoridades autonómicas.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos. ISO 10001 Gestión de la Calidad — Satisfacción del cliente — Directrices para los códigos de conducta de las organizaciones.

Por otra parte, la certificación es un procedimiento de verificación del cumplimiento por parte de una organización de un determinado estándar que debe cumplir, bien por imperativo normativo o bien por propia decisión. La certificación, en el ámbito de esta normativa, tiene las siguientes características: voluntaria, transparente y no eximente de responsabilidad. Será expedida por los organismos de certificación. Sello Europeo de Protección de Datos. Información completa. Tiempo de duración, tres años. Renovación. Retirada de la certificación y registro del Comité Europeo de Protección de Datos.

Los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informadas la Autoridad de control, a fin de esta pueda ejercer, si así se requiere.

Los mecanismos de cooperación y coherencia presentes en la normativa de protección de datos

El mecanismo de coherencia es un marco en el cual se arbitran medidas y procedimientos que se establecen entre las autoridades de control y la Comisión Europea, en base al Reglamento (UE) 2016/679 y en torno al Comité Europeo de Protección de datos.

Los temas o cuestiones que activan el dictamen del Comité Europeo de Protección de Datos vienen listados en el artículo 65 del Reglamento (UE) 2016/679, a lo cual hay que añadir las “decisiones de adecuación” que emitirá el Comité mediante dictámenes u ordenes de ejecución el artículo 45, apartado 3 del Reglamento (UE) 2016/679.

Dentro de los mecanismos de coherencia se encuentran: la norma corporativa vinculante y las cláusulas tipo.

La norma corporativa vinculante es un instrumento que el Reglamento pone a disposición de la Autoridad de control de cada Estado y que se incluye como uno de los parámetros que activan al Comité de Protección de Datos, dentro de los mecanismos de coherencia del

Reglamento y a falta de decisión de adecuación del nivel de protección emitida por el Comité Europeo de Protección de Datos.

Las normas corporativas vinculantes son "garantías adecuadas" y están dentro de los mecanismos de coherencia.

Entendemos como cláusula tipo, aquella que no ha sido objeto de la negociación individual entre las partes (Directiva 93/13/CEE).

Las cláusulas tipo, cláusulas contractuales tipo o cláusulas tipo de protección de datos, en el contexto del Reglamento (UE) 2016/679, se encuentran dentro de los mecanismos de coherencia y son garantías adecuadas para la transferencia de datos a nivel internacional fuera de la Unión Europea a falta de "decisiones de adecuación" y de "normas corporativas vinculantes".

El objetivo del Reglamento (UE) es que la Autoridad de control principal cooperará con las demás autoridades de control interesadas, dentro del consenso e intercambiando toda información pertinente.

El Considerando 133 del Reglamento (UE) 2016/679, entiende que las autoridades de control se deben ayudar una a otra en el desempeño de sus funciones y prestar asistencia mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior.

La asistencia mutua se debe entender como un mecanismo de cooperación cualificado, es decir, materializa una forma activa de cooperación y establece los mecanismos cuando esta se quiebre. Es un mecanismo de cooperación a demanda.

RÉGIMEN DE PROTECCIÓN DE DATOS RELATIVOS A LA SALUD Y EN EL ÁMBITO SANITARIO

Concepto jurídico de los datos relativos a la salud

La salud es un concepto inherente a la persona física y a todo lo que le ocurre o puede ocurrir que pueda afectar o afecte al equilibrio interno de su organismo o su mente. La Organización Mundial de la Salud se refiere a los factores determinantes en la salud y que incluyen el entorno social y económico, el entorno físico y las características individuales y los hábitos de cada uno. El derecho entiende a la salud como un bien jurídico protegido y todo lo que ello conlleva.

Las personas y los servicios sanitarios establecen diferentes estadios de esta relación, así pues, paciente hace referencia al que es atendido por un profesional de la salud, enfermo hace referencia al paciente que sufre una enfermedad y usuario de servicios sanitarios hace referencia a todos ellos e incluso a aquel que sin ser paciente

de un médico acude a un servicio de salud para cualquier cuestión personal. Datos relativos a la salud pueden proceder de centros sanitarios o no sanitarios, y de personas pacientes, enfermas o usuarias del sistema sanitario o no usuarios del sistema sanitario.

El Considerando 35 del Reglamento 2016/679 induce a entender que distingue el dato de salud de persona sana y el dato de salud de persona enferma; el dato personal en el contexto sanitario; el dato personal en el ámbito del secreto profesional sanitario; el dato personal relativo a la salud y el dato relativo a la salud; y el dato relativo a la salud junto al dato clínico y a la información clínica. Dato cualificado es aquel dato que, sin pertenecer a categoría especial de datos, se emite en un determinado escenario, situación o lugar o ante quien se obliga a secreto profesional (sanitario) adquiriendo las restricciones propias del tratamiento de los datos del artículo 9. La cualificación de un dato puede venir dada por cualquier de las vías enunciadas.

El dato relativo a la salud en el Reglamento (UE) 2016/679 se regula a través de su tratamiento, así pues, el cual prohibido por el artículo 9, prohibición regulada por el apartado 2 en sus puntos h) e i) y por el punto j). De tal forma, el artículo 9.2 dice que esta prohibición no tendrá efectos en determinadas circunstancias y en especial cuando la persona titular del dato de su consentimiento. Aunque, este consentimiento no hará falta y no habrá prohibición para el tratamiento de datos, en el punto h), tratamiento necesario para fines de médico-clínicos o su gestión y punto i) en tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas graves para la salud. Todo ello sobre la base del Derecho de la Unión o de los Estados miembros y que el tratamiento sea realizado por un profesional sanitario, en todo caso por una persona con obligación de secreto profesional o de guardar secreto. Resumiendo, las excepciones son las que se aplican en el derecho, excepciones por causa de necesidad o cuando el bien jurídico a proteger es superior al desprotegido mediante la aplicación de la excepción, en base a un contrato con un profesional sanitario o persona obligada a guardar secreto.

La Ley Orgánica 3/2018 en su disposición decimoséptima crea lo que se podría denominar el sistema de protección de datos relativos a la salud, en España, al remitir la ley a la una red normativa o sistema normativo compuesta por diez leyes.

Los datos en el sector sanitario son muy abundantes y la gran parte son datos cualificados, vistos en el capítulo.1.2.3. del Título III. Entre de ellos están los datos clínicos, en los centros sanitarios se organizan

entorno a la historia clínica, a la tarjeta sanitaria y a la receta, aunque también existen otros documentos como son los certificados, las agendas de los centros sanitarios y Conjunto Mínimo Básico de Datos (CMBD) que contienen datos de personas identificables.

El paradigma del dato personal sanitario es la historia clínica (HC), regulada por el Capítulo V (artículos 14 a 19 y artículo 11.3) de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

La historia clínica comprende el conjunto de los documentos (datos) relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

La responsabilidad de la HC recae sobre el facultativo y, en cuanto a su gestión y tratamiento; y sobre el director gerente de cada centro, con carácter general. Toda HC cuenta con un número o código identificativo. El informe de alta, compone la HC como el documento más relevante pues condensa todo el proceso. A raíz del Real Decreto 1093/2010 nacen nuevos documentos clínicos con unos datos comunes a todo el Sistema Nacional de Salud.

La historia clínica electrónica en el SNS, Real Decreto-ley 9/2011, es aquella que tiene soporte digital y sus requisitos son como mínimo los que rigen en la Ley 42/2002 y que a su vez está sujeta al Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

La receta es el documento de carácter sanitario, normalizado y obligatorio mediante el cual los profesionales legalmente facultados para ello prescriben a los pacientes los medicamentos o productos sanitarios sujetos a prescripción médica, para su dispensación por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas o, conforme a lo previsto en la legislación vigente, en otros establecimientos sanitarios, unidades asistenciales o servicios farmacéuticos de estructuras de atención primaria, debidamente autorizados para la dispensación de medicamentos. La ordenes de dispensación es la receta que pueden utilizar los profesionales de la enfermería.

El responsable de la receta es el profesional que la emite, sin embargo, será también conocida por el farmacéutico y personal de farmacia.

Las recetas del Sistema Nacional de Salud son documentos oficiales que contiene datos de los pacientes relativos a su salud y están sujetos a normativa tal como la Ley 14/1986 General de Sanidad; Real Decreto 1718/2010; Real Decreto 1718/2011; Real decreto 954/2015; Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios y al Real Decreto 1302/2018.

La recta electrónica del Sistema Nacional de Salud viene regulada por la Ley 16/2003 de cohesión y calidad del SNS; Real Decreto 1718/2010; Real Decreto 1718/2011; Real Decreto-Ley 9/2011; Real Decreto Ley 16/2012; Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios; y el Real Decreto-ley 12/2018.

La tarjeta sanitaria es un documento que acredita el derecho acceso de los ciudadanos a las prestaciones de la atención sanitaria. La tarjeta sanitaria del SNS es el documento administrativo que acredita el derecho acceso de los ciudadanos a las prestaciones de la atención sanitaria que proporciona el SNA, mediante determinados datos de su titular, con un formato único y común válido para todo el SNS y con suficiente capacidad de adaptación, en su caso, a la normalización que pueda establecerse para el conjunto de las Administraciones públicas y en el seno de la Unión Europea. Regulada por el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual (TSI) y por el Real Decreto 702/2013, de 20 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual. Contiene códigos que permiten identificar a la persona titular.

La tarjeta sanitaria europea, deriva de la aplicación de los Reglamentos de la Seguridad Social dentro de la UE. La normativa recogida en estos Reglamentos, se centra en los acuerdos entre los sistemas de seguridad social y la Directiva 2011/24/UE, no afecta a las prestaciones ya reconocidas en los mencionados Reglamentos.

La gran importancia del documento denominado TSI en toda la normativa de protección de datos personales y el riesgo de que a través de estos documentos se pueda vulnerar el RGPD viene reforzado, más si cabe, por el artículo 54. (Red de comunicaciones del Sistema Nacional de Salud) de Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

El conjunto Mínimo Básico de Datos (CMBD) supone un extracto impersonal de información administrativa y clínica, que debe ser recogida a partir del informe de alta, al que no sustituye en ningún caso y completada, si es necesario, con la HC. Contiene tipo de código de Identificación Personal, código de Identificación Personal, número de historia clínica, fecha de nacimiento y sexo, que permite su identificación. El CMBD tiene tres tipos de datos, por una parte, los datos del paciente, por otro lado, los datos de identificación del episodio (entendido como motivo de consulta o ingreso) y, por otro lado, los datos clínicos. La función básica del CMBD es la administración de y gestión de la información clínica de cada paciente, permitiendo su almacenamiento y su recuperación, además del uso para su agregación y comparación.

Principios del tratamiento de datos relativos a la salud y los derechos que hace posible la efectividad del derecho a la protección de los datos personales en el sector de la salud

En el contexto de España la protección del dato de los pacientes nace de dos fuentes de derecho. Por una parte, de la protección de los datos de carácter personal de cualquier persona (RGPD) y por la otra parte, de la regulación de la información que genera la persona cuando adquiere el rol de paciente (Ley 41/2002), que, si bien las dos normas confluyen en los datos personales relativos a la salud, cada norma actúa en base a principios distintos. Si bien es cierto que la Ley Orgánica 3/2018 en su Disposición adicional decimoséptima crea un verdadero sistema jurídico de protección de los datos relativos a la salud e incluye a la Ley 41/2002.

Esta protección de los datos de la persona actúa en dos dimensiones. En primer lugar, cualquier información concerniente a personas físicas identificadas o identificables, Ley Orgánica 3/2018 y el Reglamento (UE) 2016/679. En segundo lugar, la dimensión especial de lo que el ordenamiento jurídico incluye en la Ley Orgánica 3/2018 mediante su artículo 9, artículo 28.2, y en especial en su Disposición adicional decimoséptima sobre tratamientos de datos de salud.

El primer principio que emana del Reglamento 2016/679 es el principio de proactividad, también llamado de responsabilidad proactiva, estando asignado al responsable del tratamiento de datos. Otro principio es la protección pasiva del dato. El principio de minimización de los datos personales que aparece en el Reglamento (UE) 2016/679 mencionado en los artículos 5, 25, 47 y 89 y en el Considerando 156, goza de una especial importancia en el sector sanitario, de tal forma que no es posible hacer acopio ni tratar datos relativos a la salud de las personas por si pudiera ser necesario en un futuro y no hay ninguna excepción en este principio que emane del artículo 9.

Por otra parte, también es cierto que en el apartado 2 del mismo artículo 9, excepciona determinados supuestos de la prohibición establecida sobre el tratamiento de los datos relaticos a la salud, pero en ningún caso a la expresión se aplica a este principio sino tan solo al requisito del consentimiento.

Los principios del tratamiento de los datos relativos a la salud son: la licitud, la lealtad y la transparencia, con relación al interesado, la limitación de la finalidad, la minimización de datos, la exactitud de los datos, la confidencialidad, licitud de tratamiento, el consentimiento, el consentimiento del menor, las categorías especiales de datos, el tratamiento de los datos de naturaleza penal, el tratamiento de los datos sin identificación y otros como el principio de periodos de conservación limitados, el principio de la calidad de los datos, el principio de la protección de los datos desde el diseño y por defecto y el principio de las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes, artículo 4, Normas corporativas vinculantes, Reglamento (EU) 2016/679).

En relación al documento "Ejerce tus derechos" y en conjunción con el documento de la AEPD de noviembre de 2019 denominado "Guía para pacientes y usuarios de la Sanidad", cabe especificar que los derechos de la persona en relación a sus datos relativos a su salud o a sus relaciones con el sector sanitario se rigen por estas características:

1. Su ejercicio es gratuito y obligado salvo en caso de solicitudes "manifiestamente infundadas o excesivas especialmente debido a su carácter repetitivo".
2. Derecho a ser informado:
    a. de la identidad y nombre del responsable del tratamiento de sus datos (puede ser el médico privado, profesional sanitario de la compañía de seguro médico suscrito, hospital público o privado, o Servicio de Salud de la Comunidad Autónoma),
    b. de los datos del delegado de protección de datos, excepto las consultas privadas de un profesional sanitario,
    c. de los fines del tratamiento de sus datos y base jurídica del mismo,
    d. destinatarios se sus datos personales,
    e. intención por parte del responsable de transferir sus datos,
    f. plazo de conservación de los datos,
    g. por el responsable sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio.

3. Derecho a solicitar del responsable acceso a los datos.
4. Derecho a retirar su consentimiento en cualquier momento, sin que ello afecta a la licitud del tratamiento basado en el consentimiento previo a su retirada.
5. Derecho a presentar una reclamación ante una autoridad de control y derecho a presentar dicha reclamación ante el DPO.
6. Derecho a ser informado de la existencia y uso de decisiones automatizadas, es decir, tomadas mediante procesos informáticos sin intervención humana, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o le afecten significativamente de modo similar. El afectado tendrá derecho como mínimo a obtener información significativa sobre la lógica aplicada, así como la intervención humana, a expresar su punto de vista y a impugnar la decisión sin intervención humana, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o le afecten significativamente de modo similar.
7. Derecho a conocer ulteriores tratamientos a los que se someterán sus datos.
8. Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más
9. Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
10. Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una autoridad de control. Prorrogable a dos meses.
11. Los derechos se pueden ejercer directamente o por medio de tu representante legal o voluntario.
12. Cabe la posibilidad de que el encargado sea quien atienda tu solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule.

Los derechos del Capítulo III del Reglamento (UE) 2016/679 y el Título III de la Ley Orgánica 3/2018 son los que se describen a continuación, en consonancia con el documento de la AEPD de diciembre de 2019 sobre "Guía para pacientes y usuarios de la sanidad": la transparencia e información al afectado; el derecho de acceso: el derecho a la rectificación, el derecho a la supresión, el derecho a la limitación del tratamiento, el derecho a la portabilidad, el derecho de oposición, derecho a presentar una reclamación ante una autoridad de control, el derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento, representación de los interesados, derecho a indemnización y responsabilidad.

Tratamiento de los datos relativos a la salud en el tratamiento de categorías especiales en Reglamento 2016/679 y Ley Orgánica 3/2018

Se aplican los criterios de los elementos del tratamiento de datos que la Tesis planta con carácter general (elementos: básicos, complementarios y adicionales) a las categorías especiales de datos del Reglamento (UE) 2016/679 y Ley Orgánica 3/2018 y más concretamente a la categoría de dato relativo a la salud.

La licitud del tratamiento de datos con carácter general se consigue a través de 6 vías y las exclusiones de la prohibición del artículo 9 se subdividen en 2 grandes grupos, visto en "Tratamiento de los datos en base a la normad de protección" de las Conclusión Globales, página 460. En la Ley Orgánica 3/2018 el tratamiento de los datos relativos a la salud se encuentra en la Disposición adicional decimoséptima (Tratamiento de los datos de salud). Sistema de protección de datos.

Las exclusiones a la prohibición del tratamiento de los datos relativos a la salud se encuentran en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679.

El artículo 9 del Reglamento (UE) establece que en los supuestos relacionados con la salud el tratamiento está legitimado: por el consentimiento del interesado; cuando peligre su vida o la de un tercero; cuando intermedia una sentencia judicial; para fines de salud y asistencia sanitaria; y por razones de interés público en el ámbito de la salud pública o para garantizar la seguridad en asistencia sanitaria una vez protegidos los derechos y libertades del interesado, en particular el secreto profesional.

La Disposición adicional decimoséptima de Ley Orgánica 3/2018 trata el campo de la salud, incluyendo los datos genéticos. Trata de los datos de salud y genéticos comprendidos en; Ley 14/1986, Ley 31/1995, Ley 41/2002, Ley 16/2003, Ley 44/2003, La Ley 14/2007, Ley 33/2011, Ley 20/2015, Real Decreto Legislativo 1/2015, Real Decreto Legislativo 1/2013. Tratamiento de los datos en la investigación, se podrá dar dicho uso cuando: por consentimiento, por seudonimización y por la iniciativa parta de las autoridades sanitarias e instituciones públicas. Los supuestos de reutilización se rigen por las siguientes premisas: por consentimiento o por causa mayor. Salvo las excepciones que presenta el artículo 89 del Reglamento (UE) 2016/679.

Los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el

tratamiento de datos personales o de datos seudonimizados o anonimizados.

La historia clínica es el documento paradigmático de los datos relativos a la salud. EL tratamiento de la HC está compuesto por sus elementos básicos, complementarios y adicionales, a los cuales se debe añadir los elementos de unidad y de integración. En el Capítulo 1.2.5.1 del Título III se define que la historia clínica es un sistema de datos que comprende el conjunto de documentos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos. De la historia clínica emanan distintos documentos que si bien nacen de ella tienen distinta naturaleza y tendrán distintos tipos de tratamiento.

El tratamiento de la historia clínica: hay tres tipos de responsables; el facultativo, como responsable del dato como reflejo de su actividad asistencial; el centro sanitario (director gerente), como responsable material de la gestión del tratamiento de los datos; y la Administración pública sanitaria. El personal de administración y gestión de los centros sanitarios puede acceder a los datos de la historia clínica, aunque solo podrá acceder a los datos relacionados con sus propias funciones. También podrán tratar este tipo de datos los profesionales que ejerza funciones de inspección, evaluación, acreditación y planificación.

La receta médica es el documento de carácter sanitario con datos relativos al paciente, al medicamento, del prescriptor y otros. La receta está sometida al tratamiento del artículo 9 del RGPD. La receta vincula al paciente con un profesional, es un documento individual con dos responsables, el facultativo que lo emitió y en el caso del orden de prescripción, el enfermero/a que lo ordenó. El tratamiento de la receta se describe en base a los elementos del tratamiento: básicos, complementarios, adicionales y otros.

Tarjetas sanitarais hay muchas. La tarjeta sanitaria del Sistema Nacional de Salud es un documento administrativo con datos de su titular que posibilita el acceso de este a las prestaciones de la Seguridad Social que proporciona el Sistema Nacional de Salud. Dispone para ello de los datos básicos comunes, el código de identificación personal del Sistema Nacional de Salud y la base de datos de población protegida de dicho sistema. La utilización de la tarjeta sanitaria permite la visualización de los datos personales y al acceso de datos de salud. Le será de aplicación el Reglamento (UE) 2016/679 y la Ley orgánica 3/2018 y todas las normas de protección

que el sean de aplicación. La tarjeta sanitaria tiene un fin dentro del sector sanitario y da acceso directo a datos automatizados de naturaleza sanitaria, de salud. En consecuencia, también le es de aplicación lo dispuesto en el artículo 9 del Reglamento (UE).

La Administración Pública dispone de bases de datos de los usuarios del Sistema Nacional de Salud con tarjeta sanitaria, con información básica y situaciones de aseguramiento, cuyo fin será el de proceder a la generación del código de identificación personal del Sistema Nacional de Salud. La tarjeta sanitaria permite crear bases de datos para la Administración pública, con información del sistema de Seguridad Social y del mutualismo administrativo y que permitirán el tratamiento de datos de las situaciones de las personas respecto a altas, bajas, cobertura de prestaciones y movilidad de pacientes en la Unión Europea, de acuerdo con los reglamentos comunitarios vigentes en esta materia.

A través del Código de Identificación Personal o CIP, que está inscrito en la parte frontal delantera de la tarjeta sanitaria y está también grabado en la banda magnética de la parte dorsal trasera de la Tarjeta se puede acceder su puede interrelacionar la persona, con la Base de Datos de la tarjeta sanitaria y a su vez con el Conjunto Mínimo Básico de Datos.

El tratamiento de la tarjeta se describe en base a los elementos del tratamiento: básicos, complementarios, adicionales y otros.

La Disposición adicional decimoséptima en su punto 2, introduce dos concetos nuevos, la seudonimización y al reidentificación. La legitimación de una persona para la utilización de datos personales con fines de investigación en salud pública y/o biomedicina se produce a través de la seudonimizados o del consentimiento. A lo que hay que añadir: una separación técnica y funcional; y un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación. La Ley Orgánica 3/2018 autoriza expresamente la reidentificación de los datos cuando exista un peligro real y concreto para la seguridad o salud de una persona o grupo de personas.

El uso de datos personales seudonimizados deberá ser sometido al informe previo del comité de ética. En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un DPO o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que

comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados

Se esta forma la base jurídica del tratamiento de los datos relativos a la salud protegido por el artículo 9, cuando el interesado no haya hecho manifiestamente públicos estos datos, corresponde a personas:

1. que estén en poder del consentimiento,
2. en actividad sanitaria, sujetas a la obligación de secreto profesional,
3. obligadas al tratamiento de tales datos cuando sean necesarios para:
    a. el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado, en el ámbito del Derecho laboral y de la seguridad y protección social,
    b. en el supuesto de que el interesado incapacitado para dar su consentimiento, proteger intereses vitales del interesado o de otra persona física,
    c. cuando los tribunales actúen en ejercicio de su función judicial,
    d. razones de un interés público esencial,
    e. razones de interés público en el ámbito de la salud pública,
    f. con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1.

De esta forma pueden tratar los datos relativos a artículo 9.2. del Reglamento (EU) 2016/679, los que estén obligados al secreto profesional, cuando el ámbito es el entorno asistencia, clínico o médico, o las personas que estén en una de las siguientes situaciones, en base al artículo 6.1 del Reglamento (EU) 2016/679:

1. poseer el consentimiento del interesado
2. tener que ejecutar un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales
3. para cumplir una obligación legal del responsable del tratamiento
4. para proteger intereses vitales del interesado o de otra persona física
5. para una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento
6. 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.

Lo cual significa que si hubiera algún tratamiento de datos relativos a la salud que no se acogiera a alguna exclusión del artículo 9.2, no se podría aplicar el artículo 6.1 de legitimación para el tratamiento, y

nadie estaría legitimado para tratarlo. Este es el caso de las historias clínicas en archivos pasivos o datos en las historias clínicas no necesarios para atender a la salud actual de la persona, además no útiles para procesos de investigación o fuera de ellos.

La AEPD publicó un informe sobre los tratamientos de datos en relación con el COVID-19 el cual manifiesta que "el RGPD contiene reglas necesarias para permitir legítimamente tratamiento de datos personales en situaciones de emergencia sanitaria".

El Considerando 46 Reglamento (UE) 2016/679 hace mención a las pandemias. Las situaciones de excepción que aparecen en el artículo 9 del Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018 contemplan como supuestos de activación, las crisis en salud pública, en consecuencia, se deben incluir las alertas sanitarias producidas por una epidemia o pandemia, sin embargo, en base al Considerando 45 del Reglamento (UE) 2016/679 deberán constar en el Derecho de la Unión o de los Estados miembros.

El Gobierno de España declara el Estado de Alarma a través del Real Decreto 463/2020 y lo mantiene durante el primer semestre de 2021 en base al Real Decreto 926/2020. Las limitaciones que obliga el Real Decreto 926/2020, afectan de lleno a los derechos fundamentales de la CE, y de forma explícita estas restricciones son:

1. Limitación de la libertad de circulación de las personas en horario nocturno. (artículo 5)
2. Limitación de la entrada y salida en las comunidades autónomas y ciudades con Estatuto de autonomía. (artículo 6)
3. Limitación de la permanencia de grupos de personas en espacios públicos y privados. (artículo 7)
4. Limitación a la permanencia de personas en lugares de culto. (artículo 8)

La Autoridad de control dentro de la protección de datos del sector de la salud

La Autoridad de control tiene, entre sus diversas funciones, las de asesorar a las instituciones, también a las sanitarias públicas y privadas, sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.

La Autoridad de control, en el ámbito sanitario, podrá llevar a cabo investigaciones en forma de auditorías de protección de datos, obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones y obtener el acceso a todos los locales del

responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos.

La primera relación que el Reglamento (UE) establece entre la Autoridad de control y el dato relativo a la salud, es precisamente en la EIPD, ver página 210.

La segunda relación que el Reglamento (UE) establece entre la Autoridad de control y el dato relativo a la salud, se manifiesta en el supuesto relativo a la consulta previa, por un responsable del tratamiento de datos.

La tercera relación que el Reglamento (UE) establece entre la Autoridad de control y el dato relativo a la salud, viene a través de la garantía que deberá dar el Gobierno, en todo caso, de que la Autoridad de control sea consultada durante la elaboración de toda propuesta de medida legislativa o de una medida reglamentaria que se refiera al tratamiento, artículo 36.4 del Reglamento (UE) 2016/679, y según se desprende del RGPD, en especial en los supuestos del artículo 9.

Responsable y encargado del tratamiento en sector de la salud

En base al artículo 4.7) del RGPD el responsable del tratamiento o responsable "es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento". También puede haber corresponsables del tratamiento. El responsable del tratamiento será responsable del cumplimiento de los principios relativos al tratamiento, dispuesto en el apartado 1 del artículo 5 del Reglamento (UE) 2016/679, y deberá ser capaz de demostrarlo, en base al principio de responsabilidad proactiva del Considerando 85 del Reglamento (UE) 2016/679 aplicando las máximas garantías.

El artículo 37 del Reglamento (UE) 2016/679 dice que deberá ser nombrado un DPO por el responsable o encargado de una organización en la cual las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9.

En cuanto a la historia clínica, la Ley 41/2002 establece la jerarquía de responsable del tratamiento o del fichero de la historia clínica. Por otra parte, en cuanto a la receta, tiene dos responsables, el facultativo y el farmacéutico de la oficina de farmacia, pero no implica que compartan la corresponsabilidad del artículo 26 del Reglamento (UE) 2016/679, dado que son dos responsabilidades distintas, aunque sobre un mismo documento o conjunto de datos.

El responsable del tratamiento de la tarjeta sanitaria es todo directivo de cualquier organización que utiliza para llevar a cabo su actividad corriente el tratamiento de los datos de las tarjetas sanitarias, en cualquiera de sus formas, es decir, por ejemplo los directores de los hospitales o los responsables de los Centros de atención sanitaria en general y los responsables de las Administraciones Públicas o en las empresas privadas encargadas del mantenimiento de las Bases de Datos de Población Protegida del Sistema Nacional de Salud o de las bases de los asegurados en las compañías privadas.

Las personas que suministren sus datos personales a las organizaciones o personas que los necesiten para el ejercicio de su actividad tendrán derecho a conocer la identidad y los datos de contacto del responsable y, en su caso, de su representante, artículo 13.1 del RGPD.

La norma no distingue entre sector público o sector privado al definir al responsable, de forma explícita, sin embargo, parece que la interpretación de ciertos artículos del Reglamento (UE) 2016/679 permite esta diferenciación. A criterio de la Agencia Española de Protección de Datos, ciertas "cláusulas comodín" o cláusulas que excepcional la regla, también lo permiten.

Esta situación, indefinición del RGPD en el sector público de la salud, es aclarada por la Ley Orgánica 3/2018 cuando en su artículo 34 determina con más precisión las organizaciones que deben tener DPO.

Todos los centros sanitarios que utilicen historias clínicas, recetas o tarjetas sanitarias tienen un responsable del tratamiento de datos, incluso, aunque la organización no lo tenga identificado, pues como dice el artículo 4.y) del Reglamento (UE) 2016/679 hay un responsable del tratamiento de datos cuando se utilizan datos personales y se tratan, siendo el responsable del tratamiento el que los define y determina los medios para su tratamiento.

El tratamiento de la tarjeta sanitaria no es un escenario específico del sector público. En el sector público se incluyen como responsables a todos los directores de los hospitales, a los directores de las Fundaciones de Investigación de los hospitales públicos, a los responsables de los Centros de Atención primaria y a los responsables de las unidades de mantenimiento de las Bases de Datos de Población Protegida del Sistema Nacional de Salud.

El sector privado no tiene ningún tipo de particularidad en cuanto a la aplicación del RGPD. La Agencia Española de Protección de Datos es la Autoridad de control principal en España en relación al artículo 51 del Reglamento (EU) 2016/679. Esta Agencia publicó en el mes de noviembre de 2019 la Guía para pacientes y usuarios de la sanidad. Establece una excepción en la necesidad u obligatoriedad del

consentimiento del paciente o usuario, lo cual la AEPD entiende que se sustenta en el apartado 6.1.b) es de aplicación a las compañías aseguradoras de salud privadas y que el apartado 6.1.c) es de aplicación para la sanidad pública.

La fortuna o la poca fortuna de la aplicación de esta "cláusula comodín" del Reglamento (UE) 2016/679 para la no aplicación de una o varios principios o normas de protección indica que el RGPD permite interpretar diferencias entre el sector público y el privado.

El Reglamento (UE) 2016/679 define en su artículo 4.8 al encargado del tratamiento diciendo que "encargado del tratamiento o encargado es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento." No distinción entre el sector público ni el privado.

El delegado de protección de datos (DPO) en el sector de la salud

El delegado de protección de datos es el garante del cumplimiento de la normativa de protección de datos en las organizaciones, garante interno, sin sustituir las funciones que desarrolla la Autoridad de control, como garante externo.

Un centro sanitario es siempre subsidiario de disponer de delegado de protección de datos, si bien se exceptúan los profesionales de la salud que ejerzan su actividad a título individual. Bien sea por el artículo 37.1.a) y 37.1.c) del Reglamento (UE) 2016/679, bien sea por el análisis de las figuras de responsable y encargado del tratamiento de datos o bien sea por el contenido explícito del artículo 34.1.L) de la Ley Orgánica 3/2018, todo ello en su conjunto nos lleva a entender que, en cada centro asistencial público deberá haber un DPO o alguien que haga sus funciones, en las condiciones que indica tanto el Reglamento (UE) 2016/679 como la Ley Orgánica 3/2018. También están obligados los centros privados en base al artículo 37.1.c) del Reglamento (UE) 2016/679 y al artículo 34.1.L) de la Ley Orgánica 3/2018.

Las sanciones de las infracciones se rigen por el artículo 76 de la Ley Orgánica 3/2018 y por los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679.

Las exigencias en el sector público son superiores en cuanto a la obligatoriedad del DPO. En el sector privado aparecen una serie de peculiaridades:

- Se excluyen los tratamientos a pequeña escala. El Reglamento está haciendo mención de que tan solo las organizaciones sanitarias en donde trabajan profesionales de la salud por cuenta ajena están obligadas a nombrar y contratar un DPO.

En este orden de cosas, la Ley Orgánica 3/2018 en su artículo 34 viene a expresar lo mismo.

- Nada dice el RGPD ni la Ley Orgánica 3/2018 de las oficinas de farmacia, que si bien no están obligadas el mantenimiento de historias clínicas utilizan la tarjeta sanitaria del paciente y tienen acceso a las recetas de los pacientes.

  El artículo 1 de la Ley 16/1997, de 25 de abril, de regulación de servicios de las oficinas de farmacia define a las oficinas de farmacia como establecimientos sanitarios privados de interés público. En base al artículo 9 del RDPG la Oficina de Farmacia está sujeta al RGPG, pero al no tratar datos a gran escala parece que no estaría obligada a disponer de DPO.

  En base al artículo 25 del Reglamento (UE) 2016/679, al principio de proactividad, artículo 5.2 del Reglamento (UE) 2016/679, que impulsa el RGPD y en base a la libertad de designación de PDO, artículo 37.4 del Reglamento (UE) 2016/679, en supuestos no obligados, se entiende que las oficinas de farmacia deberían disponer, es decir, contratar los servicios de un DPO, aunque fuera a tiempo parcial, comunicándolo a la AEPD. Sin duda esta cuestión nada clara, requiere el pronunciamiento de la AEPD.

En cuanto a las tarjetas sanitarias, todos los centros en donde se traten sus datos deberían tener un DPO, en el caso de los centros pequeños, se les aplicaría lo dicho para las oficinas de farmacia y en el caso de las compañías de seguros con Bases de Datos de asegurados y en los centros con Bases de Datos de Población Protegida del SNS, deberían disponer de DPO, en todo caso.

Cuando los centros de investigación tengan una actividad a gran escala, en base al artículo 37.1.c) del Reglamento (UE) 2016/679, deberán disponer de DPO.

Un ejemplo de la aplicación indebida del RGPD en cuanto a la designación del DPO es la Consejería de Sanidad de la Comunidad de Madrid que en vez de designar en DPO en cada centro sanitario obligado nombró un DPO para todos los centros, ubicándose en los servicios centrales de la Consejería, creando un Comité Delegado de Protección de Datos. Es preciso hacer notar que la AEPD mediante la resolución PS/00417/2019 de 9 de junio de 2020 sancionó a la empresa GLOVOAPP23, S.L. por infracción graves por no disponer de delegado de protección de datos a pesar de que la empresa alega disponer de un Comité de Protección de Datos.

EL DELEGADO DE PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO DE LA SANIDAD

La identificación de responsables del tratamiento en el sector público de la salud

La identificación correcta del responsable del tratamiento es una de las premisas de la protección de los datos de las personas, además también es una forma para evitar lo que ha ocurrido en relación con la aplicación del Reglamento (UE) 2016/679 y la Ley orgánica 3/2018 en la sanidad pública, capítulo 6.3., del Título III, página 420.

El responsable del tratamiento es quien debe aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, artículo 4.7) del Reglamento (UE) 2016/679, frente a los interesados y ante las autoridades de supervisión, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas.

Se debe identificar al responsable del tratamiento de los datos de la tarjeta sanitaria en cuanto a la base de datos y al responsable del tratamiento de datos de todos los establecimientos en donde se utiliza la tarjeta sanitaria. Así pues, el responsable de la historia clínica y el de la tarjea sanitaria pueden coincidir en los centros obligados al mantenimiento de las historias clínicas de los pacientes, pero también puede haber centros en los que se trate la información de la tarjeta sanitaria y que en el mismo centro no estén obligados al mantenimiento de la historia clínica, aunque si acceso a la historia clínica electrónica, por ejemplo, los centros de Atención primaria.

Una vez detectados los responsables del tratamiento de los datos relativos a la salud de las personas de las organizaciones cuya actividad se sustenta en estos datos y en su tratamiento, se debe analizar si este responsable debe nombrar a un DPO o sin estar obligado a ello, es conveniente que lo nombre.

Cabe destacar que una misma fuente de datos puede tener varios responsables del tratamiento, tal es el caso de los datos personales relativos a la salud. Por una parte, estos datos van a la historia clínica, por otra a la receta y por otra a la tarjeta sanitaria, todos ellos con sus tratamientos específicos y destinados a actividades distintas, todos ellos con distintos responsables y en algún caso con corresponsables.

Resumen, pasos a seguir para la identificación del responsable del tratamiento de datos:

1.º Identificar datos y tipos de datos registrados o a registrar
2.º Identificar tipo de actividad a los que corresponden los datos que se registran y cuál es el fin de dicho registro
3.º Identificar tipo de tratamiento

4.º Identificar la organización que hace posible la actividad y que trata los datos

5.º Identificar los niveles de responsabilidad, bien de forma deductiva o bien acudiendo a la norma, en su caso

6.º Identificar al responsable del tratamiento de datos o el responsable principal y los corresponsables, en su caso

7.º Identificar las obligaciones del responsable del tratamiento de datos en base al tipo de datos, tipo de tratamiento, volumen del tratamiento y tamaño de la organización

El delegado de protección de datos en la protección de los principios del RGPD y la aplicación del derecho a la protección de la salud en el sector público de la salud

En base al artículo 39 RGDP el DPO, tal como se ha descrito en el capítulo 4.1.5 del Capítulo II, tiene unas atribuciones y funciones determinadas.

En relación a la protección de los principios del RGPD, en el sector público de la sanidad el DPO realizará asesoramiento general en todo lo relativo a los principios y obligaciones que impone el Reglamento (UE) 2016/679. De tal forma deberá realizar supervisión y auditorías del cumplimiento de los principios del Reglamento (UE) 2016/679, de las políticas en materia de protección de esos principios, así como de la concienciación y formación del personal implicados y obligados por la normativa. También deberá elaborar informes de evaluación de impacto sobre los principios de ciertos tratamientos de datos personales del artículo 35.b) del Reglamento (UE) 2016/679.

El DPO deberá supervisar y auditar la observancia y el respeto de los principios del tratamiento de los datos relativos a la salud, que se reflejan en al capítulo 2.1. del Título IV, página 429. El DPO deberá presta a tención a los principios del tratamiento de los datos relativos a la salud son: la licitud, la lealtad y la transparencia, con relación al interesado, la limitación de la finalidad, la minimización de datos, la exactitud de los datos, la confidencialidad, licitud de tratamiento, el consentimiento, el consentimiento del menor, las categorías especiales de datos, el tratamiento de los datos de naturaleza penal, el tratamiento de los datos sin identificación y otros como el principio de periodos de conservación limitados, el principio de la calidad de los datos, el principio de la protección de los datos desde el diseño y por defecto y el principio de las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes, artículo 4, Normas corporativas vinculantes, Reglamento (EU) 2016/679).

El DPO deberá supervisar y auditar la aplicación de los derechos en la protección de datos el RGPD visto en el capítulo 2.2. del Título IV,

página 433. El DPO deberá estar al documento "Ejerce tus derechos" y en conjunción con el documento de la AEPD de noviembre de 2019 denominado "Guía para pacientes y usuarios de la Sanidad". Además vigilará los derechos que proclaman el Capítulo III del Reglamento (UE) 2016/679 y el Título III de la Ley Orgánica 3/2018 son los que se describen a continuación: La transparencia e información al afectado; el derecho de acceso: el derecho a la rectificación, el derecho a la supresión, el derecho a la limitación del tratamiento, el derecho a la portabilidad, el derecho de oposición, derecho a presentar una reclamación ante una autoridad de control, el derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento, representación de los interesados, derecho a indemnización y responsabilidad.

El delegado de protección de datos y el tratamiento de los datos en el sector público de la salud

Con carácter general y en relación a los datos protegidos por el artículo 9 del Reglamento (UE), el DPO deberé supervisar y auditar la efectividad de los derechos que garantiza el RGPD y recordar al responsable del tratamiento será él quien deberá demostrar que han sido respetados.

Por otra parte, el DPO en España tiene una función muy relevante en cuanto puede ser fuente de resolución de reclamaciones contra el responsable del tratamiento de los datos.

Además de resolver las reclamaciones que interpongan las personas legitimadas, en base al artículo 37 y al artículo 65.4 de la Ley Orgánica 3/2018.

Como se ha visto en el capítulo 5.6.4 del Título I que el Estado de Alarma por la pandemia COVID-19 iniciada en marzo de 2020, por motivos de salud pública, activa una serie de excepciones en el tratamiento de los datos de las personas con carácter general, sin embargo, todas estas solo afectan al principio del consentimiento para el tratamiento de los datos personales, del artículo 6 del RGPD, y para el artículo 9.2 del RGPD. Estas excepciones no afectan al resto de principios vistos en el capítulo 3.1. del Título I y capítulo 2.1. del Título III, ni a los derechos descritos en el capítulo 4.1. del Título I y capítulo 2.2 del Título III.

El importante rol del PDO tratado en el capítulo 2.1 y capítulo 2.2 del Título IV se hace todavía más necesario a raíz de la situación excepcional que plantea el Estado de Alarma, por causa de salud pública, en relación a ciertos conflictos que han emergido, a raíz de las medidas de gestión de la pandemia, entre algunos derechos fundamentales entre sí y con algunos bienes jurídicamente protegidos, el derecho a la protección de datos, el derecho a la protección de la salud y el derecho a la libre movilidad dentro de la UE.

La gestión de la pandemia ha demostrado que se pueden poner en conflicto derechos fundamentales y bienes jurídicamente protegidos, lo cual hace más necesaria la figura del DPO con el fin de facilitar que el ciudadano y el profesional conozcan a quién consultar, con facilidad y eficacia, en caso de duda sobre las medidas que se van adoptando de los centros sanitarios y la imperiosa necesidad de facilitar que los poderes públicos respeten todo el contexto de los derechos fundamentales visto en el capítulo 2.3 del Título I sin tener que acudir a los tribunales, circunstancia que hacen penosas e ineficaces las garantías constitucionales.

Uno de los ejemplos de ello son casos que se analizan en el capítulo 5.6.5 del Título I, en concreto las recomendaciones de la Comisión Europea y los supuestos tratados en el capítulo 3.5 del Título III, del cual llama la atención el último de ellos, el supuesto del pasaporte o carnet de inmunidad del COIVD-19. Tras mucho debate, la Comisión Europea anunció en el mes de marzo de 2021 la elaboración de un reglamento propuesta sobre un marco para la emisión, verificación y aceptación de certificados de interoperabilidad de vacunación, Certificado Verde Digital, básicamente para evitar los obstáculos a la movilidad que puede suponer que cada Estado miembro genere sus propios certificados sin contar con los certificados del resto de Estados miembros.

Por la gran confusión generada, la Comisión Europea emitió un comunicado en su página web el día 17 de marzo de 2021: “Mediante el certificado digital verde adoptamos un planteamiento europeo para que los ciudadanos de la UE y sus familiares puedan viajar con seguridad y con el mínimo de restricciones este verano. El certificado digital verde no será un requisito previo para ejercer el derecho a la libre circulación y no discriminará de ningún modo”. Finalmente, la Comisión de la Unión Europea publica en su página web el día 20 de mayo de 2021 el “Certificado COVID Digital de la UE: el Parlamento Europeo y el Consejo alcanzan un acuerdo sobre la propuesta de la Comisión”, a lo cual añade: “La Comisión acoge con satisfacción el acuerdo político provisional alcanzado hoy entre el Parlamento Europeo y el Consejo sobre el Reglamento que regulará el Certificado COVID Digital de la UE”.

Tras el acuerdo alcanzado por el Parlamento Europeo y el Consejo, el Certificado COVID Digital de la UE, según el comunicado de la Comisión: “abarcará la vacunación, los tests y la recuperación; estará disponible en formato digital y en papel, dependiendo de la elección de cada persona destinataria, e incluirá un código QR firmado electrónicamente; será gratuito, fácil de obtener y también podrán disponer de él las personas vacunadas antes de la entrada en vigor del Reglamento que lo regule; los Estados miembros también lo podrán utilizar con fines nacionales, en función de sus respectivas legislaciones; los Estados miembros se abstendrán de imponer restricciones adicionales de viaje a las personas titulares de un Certificado COVID Digital de la UE, a menos que dichas restricciones sean necesarias y proporcionadas para salvaguardar la salud

pública; la Comisión también movilizará 100 millones de euros para proporcionar tests asequibles a los Estados miembros.

El Parlamento Europeo y el Consejo deben adoptar ahora formalmente el acuerdo político. El Reglamento entrará en vigor el 1 de julio, con un período de introducción progresiva de seis semanas para la expedición de certificados en aquellos Estados miembros que necesiten más tiempo.

El Reglamento (UE) 2016/679 en sus Considerandos 77 y 97 presenta al DPO como una garantía de que se está aplicando correctamente el RGPD mediante su supervisión de las observancias internas del Reglamento (UE) por parte de responsables y encargados. Una situación especial de salud pública que legitima la activación de excepciones a los principios del Reglamento (UE) 2016/679, hace más evidente e importante la presencia del delegado de protección de datos en todos los ámbitos en donde la ley obliga su presencia y en especial en los centros que lleven a cabo tratamientos de datos relativos al artículo 9 del Reglamento (UE) 2016/679.

UNA PROPUESTA PARA LA CORRECTA APLICACIÓN DE LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO DE LA SANIDAD EN ESPAÑA

Un modelo de aplicación

El primer paso es la descripción del escenario, su definición, su naturaleza y la identificación de tratamientos de datos que lleva a cabo, capítulo 3.3.2 del Título III.

Delegado de protección de datos en la sanidad pública de la Comunidad de Madrid, coordinación y el manual de protección de datos

El siguiente paso es identificar la responsable y/o encargado del tratamiento de datos, capítulo 1 del Título III. Por último, analizar la organización a estudio, básicamente su estructura, tamaño y volumen de operaciones.

Establecer un nivel de coordinación entre todos los DPO de los centros sanitarios mediante una Comisión Central de PDO.

Elaborar un Manual de protección de datos de la institución pública que asegure un tratamiento homogéneo en los centros dependientes y mantener el principio de equidad e igualdad frente a la ley de las personas que acuden a dichos centros.

2. Conclusiones finales

1º. El Reglamento (UE) 2016/679 es la norma de la Unión Europea que directamente regula el derecho a la protección de los datos personales de las personas físicas en lo que respecta al tratamiento de datos y a la libre circulación de estos datos. Una norma cuyo fin es superar las dificultades armonizadoras de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

2º. En España la adaptación al Reglamento general de protección de datos requiere la elaboración de una nueva ley orgánica que sustituyera a Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal dando pie a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3º. El derecho a la protección de datos es un derecho fundamental tanto en España, a través de la Constitución, como en la Unión Europea, a través de la Carta de Derechos Humanos de la Unión Europea. El análisis de la norma RDPG y de la Ley Orgánica hay que realizarlo desde la perspectiva de la regulación de los derechos fundamentales, que si bien no son derechos absolutos están fuertemente protegidos.

4º. Principios del RGPD, son: la licitud, la Lealtad y la transparencia, la limitación de la finalidad, la minimización de los datos, la exactitud de los datos, la confidencialidad, la licitud de tratamiento, el consentimiento, el consentimiento del menor, las categorías especiales de datos, el tratamiento de los datos de naturaleza penal y el tratamiento de los datos sin identificación. Otros principios: periodos de conservación limitados, calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento y los requisitos para las transferencias internacionales.

5º. El principio de minimización prevalece sobre otros principios (AEPD, 2019) (TJUE, 2008).

6º. Los derechos presentes en el RGPD para la efectividad sus fines, son: la transparencia e información al afectado, el derecho de acceso, el derecho a la rectificación, el derecho a la supresión, el derecho a la limitación del tratamiento, el derecho a la portabilidad y el derecho de oposición. Otros derechos, Reglamento (UE) 2016/679: derecho a presentar una reclamación ante una autoridad de control; el derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento; representación de los interesados, y derecho a indemnización y responsabilidad.

7º. Organización y procedimientos en el tratamiento de datos en el RGPD:

1. Organización mediante los órganos de control:

- Comisión Europea.
- Comité Europeo de Protección de datos.
- Supervisor Europeo de Protección de Datos.
- Autoridad de control de los Estados miembros.
- Responsable y encargado del tratamiento.
- Delegado de Protección de Datos.

2. Procedimientos:
    a. La autorregulación en la protección de datos:
        - Códigos de conducta.
        - Certificaciones y organismo de certificación.
        - Sello europeo de protección de datos.
    b. Los mecanismos de cooperación y coherencia:
        - Decisión de adecuación.
        - Norma corporativa vinculante.
        - Cláusulas tipo.
        - La asistencia mutua.
    c. La Protección del diseño.
    d. La Evaluación del Impacto en la Protección de Datos Personales.
    e. El registro de actividades del responsable del tratamiento.
    f. La notificación de una violación de seguridad.
    g. La consulta previa en el RGPD.
    h. La auditoría preventiva de la Ley Orgánica 3/2018.
    i. Los procesos de seudonimización o anonimización de la Ley Orgánica 3/2018.
    j. La reclamación frente al Delegado de Protección de datos.
    k. La reclamación.

8º. Régimen del tratamiento de datos en el RGPD.

1. El RGPD hace referencia a todo tipo de datos independientemente de su soporte o tecnología.
2. El dato personal es aquel dato que permite identificar o permite ayudar a la identificación de una persona.
3. Tipos de datos en el RGPD:

a. Los que no incluye (anónimos o no identificadores personales)

b. Los que incluye:

I. Los datos personales

II. Las categorías especiales de datos (artículo 9 del Reglamento)

4. Licitud en el tratamiento de datos en el RGPD

a. De los datos personales, mediante el artículo 6

b. De las categorías especiales de datos, solo en los casos de las excepciones de prohibición, en artículo 9.2 y 9.3

5. El tratamiento de datos, régimen general: los tres niveles del tratamiento (básico, complementario y adicional).

El tratamiento de datos recoge cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no (artículo 4 RGPD). Se compone, en primer lugar, de elementos básicos, los que aparecen en el artículo 4 del RGPD, en segundo lugar, de elementos complementarios, los que no aparecen en el artículo 4 del RGPD pero son operaciones previas al tratamiento de datos o las operaciones colaterales al tratamiento de datos necesarias para que este sea lícito, y, en tercer lugar, elementos adicionales, las acciones u operaciones no básicas ni complementarias que se deben realizar o pueden realizar sobre los datos personales y que están reflejadas de alguna forma tanto en el Reglamento de la (UE) 2016/679 como en la Ley Orgánica 3/2018.

9º. Régimen del tratamiento de datos relativos a la salud en el RGPD.

Salud: el equilibrio de las funciones del cuerpo humano y/o su mente.

Los datos relativos a la salud son datos de categorías especiales y se regulan por el artículo 9 del RGPD.

a. El Considerando 35 del Reglamento 2016/679 lleva a la consideración de que se distingue el dato de salud de persona sana y el dato de salud de persona enferma; el dato personal en el contexto sanitario; el dato personal en el ámbito del secreto profesional sanitario; el dato personal relativo a la salud y el dato relativo a la salud; y el dato relativo a la salud junto al dato clínico y a la información clínica.

b. Dato cualificado: aquel dato que, sin tener una naturaleza especial o sin pertenecer a ninguna categoría especial de datos que lo haga susceptible de ser considerado un dato de tratamiento prohibido, se emite en un determinado escenario, situación o lugar y pasiva, o por ser causa que obliga a una tercera persona al secreto profesional (sanitario), se por este hecho adquiere las restricciones propias del tratamiento de los datos de categoría especial del artículo 9 del Reglamento atribuibles a los datos relativos a la

salud. La cualificación de un dato puede venir dada por cualquier de las vías enunciadas.

c. La prohibición del tratamiento de datos personales relativos a la salud. El tratamiento de las categorías especiales del artículo 9 está prohibido. El artículo 9.2 excluye de la prohibición determinadas circunstancias, es decir, siguen siendo datos de categoría especial pero que un factor ajeno permite su tratamiento.

d. Excepciones a la prohibición del tratamiento de datos personales relativos a la salud. La exclusión de la prohibición afecta tan solo al principio del consentimiento, no afectando al resto de principios. Las exclusiones se dan en base a: 1. Circunstancias que afectan a la persona física, afectado o tercero: cuando el interesado haya hecho públicos sus datos personales; cuando haya consentimiento, no se otorga al consentimiento un valor absoluto; y cuando es necesario para fines de relativos a la salud; 2. Circunstancias ajenas a la persona afectada: a. atribuidas por funciones de potestad; b. afectadas por el interés general; y c. otras.

e. El caso especial de la excepción del "interés público". El artículo 9.2.g) cita "interés público esencial" como una excepción a la prohibición, sin embargo, debe entenderse como un interés general reforzado en base a la STC de 2019 y a la STJUE de 2014.

f. Las excepciones permiten el trabamiento de los datos protegidos por el artículo 9 cuando estas excepciones estén reguladas por el derecho de la Unión o del estado miembro.

g. Solo podrán tratar los datos del artículo 9, los profesionales sujetos a la obligación de secreto profesional, o bajo su responsabilidad y cualquier otra persona sujeta también a la obligación de secreto. Este concepto es tratado por la Tesis como "secreto profesional sobrevenido".

h. En el supuesto de las recetas públicas emitidas por el Sistema Nacional de Salud, el consentimiento se podría obviar en consideración del apartado 2.h) del artículo 9. En el caso de las recetas privadas la situación es distinta y no hay soporte legal para obviar el consentimiento.

El tratamiento de datos relativos a la salud: este tratamiento sigue los tres niveles del régimen general del tratamiento de los datos, al cual se le incorpora un nivel correspondiendo a "Otros elementos del tratamiento distintos de los encontrados en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018"

10º. Los órganos de control en el tratamiento de datos relativos a la salud en el RGPD.

1. La Autoridad de control. Tres relaciones principales con el ámbito sanitario:

   a. En la Evaluación del Impacto relativas a la protección de estos datos.

   b. La consulta previa realizada por un responsable del tratamiento de datos.

c. La garantía que deberá dar el Gobierno de que la Autoridad de control sea consultada durante la elaboración de toda propuesta de medida legislativa o de una medida reglamentaria que se refiera al tratamiento, artículo 36.4 del Reglamento (UE) 2016/679, y según se desprende del RGPD, en especial en los supuestos del artículo 9

2. El responsable del tratamiento de datos:

   a. En el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9, deberá nombrar a un delgado de protección de datos.

   b. En cuanto a la historia clínica y la tarjeta sanitaria, responsable del tratamiento, es todo directivo de cualquier organización que utiliza el tratamiento de estos datos para llevar a cabo su actividad corriente.

   c. El registro y acceso a los datos de la tarjeta sanitaria clínica deberá estar sujeto en algún momento al consentimiento de la persona y a la información por parte del responsable del tratamiento de los tratamientos a los que se puede someter dichos datos.

   d. En cuanto a la receta, hay dos responsables, el profesional sanitario (médico, odontólogo o personal de enfermería), en el momento de expedir la receta y el farmacéutico de la oficina de farmacia, pero no implica que compartan la corresponsabilidad del artículo 26 del Reglamento (UE) 2016/679, dado que son dos responsabilidades distintas, aunque sobre un mismo documento o conjunto de datos.

   e. En las recetas tengan el soporte que tengan, debe entenderse que es de aplicación el artículo 9.2 y 9.3 del Reglamento (UE) 2016/679 dado que la Ley 3/2018 no las menciona en su Disposición adicional 17ª.

   f. En el sector privado, el sector de las farmacias, hay distinción en relación al tratamiento de los datos suministrados por recetas electrónicas y por recetas manuales en cuanto al consentimiento de la persona.

   g. La norma no distingue entre sector público o sector privado al definir al responsable, de forma explícita, sin embargo, parece que la interpretación de ciertos artículos del Reglamento (UE) 2016/679 permite esta diferenciación. A criterio de la Agencia Española de Protección de Datos, ciertas “cláusulas comodín” o cláusulas que excepcional la regla, también lo permiten. La Agencia Española de Protección de Datos público en el mes de noviembre de 2019 la Guía para pacientes y usuarios de la sanidad. Establece una excepción en la necesidad u obligatoriedad del consentimiento del paciente o usuario, lo cual la AEPD entiende que se sustenta en el apartado 6.1.b) es de aplicación a las compañías aseguradoras de salud privadas y que el apartado 6.1.c) es de aplicación para la sanidad pública. La fortuna o la poca fortuna de la aplicación de esta “cláusula comodín” del

Reglamento (UE) 2016/679 para la no aplicación de una o varios principios o normas de protección indica que el RGPD permite interpretar diferencias entre el sector público y el privado.

11º. La pandemia de COVID-19 en los años 2020 y 2021. La pandemia declarada por la OMS en marzo de 2020 y la gestión de la misma por los Gobiernos ha representado una prueba de estrés tanto de los propios sistemas sanitarios como de la normativa relativa a la protección de datos.

1. La pandemia del COVID-19 causa en 2020 una Alarma Sanitaria, las medidas que se deben adoptar provocó la declaración de un Estado de Alarma. En España hubo tres, el Real Decreto 463/2020, Real Decreto 900/2020 y el Real Decreto 926/2020 que mantiene el Estado de Alarma hasta mayo de 2021. Las limitaciones que obliga el Real Decreto 926/2020, afectan de lleno a los derechos fundamentales de la CE, y de forma explícita estas restricciones son:
    - Limitación de la libertad de circulación de las personas en horario nocturno. (artículo 5)
    - Limitación de la entrada y salida en las comunidades autónomas y ciudades con Estatuto de autonomía (artículo 6)
    - Limitación de la permanencia de grupos de personas en espacios públicos y privados. (artículo 7)
    - Limitación a la permanencia de personas en lugares de culto (artículo 8)
2. Se ha dado varios supuestos en los cuales ha aflorado un conflicto entre diversos derechos fundamentales:
    - Las prórrogas del Estado de Alarma
    - El estudio de la movilidad de las personas
    - El supuesto de la toma de temperatura
    - El supuesto de la realización de test del COVID-19 como detector de infectados para acceder al puesto de trabajo dentro del RGDP
    - El Supuesto del pasaporte o carne de inmunidad del COVID-19 dentro del RGPD

12º. El delegado de protección de datos en el sector de la sanidad

1. La identificación del responsable permite identificar los tratamientos de datos que requieren delegado de protección de datos.
2. La relevancia del delegado de protección de datos en el sector de sanitario viene determinada tanto por el RPDG como por las necesidades del propio sector sanitario y la característica de los datos relativos a la salud.
3. La relevancia del DPO en el sector de la sanidad:

a. El DPO deberá prestar atención a los principios del tratamiento de los datos relativos a la salud son: la licitud, la lealtad y la transparencia, con relación al interesado, la limitación de la finalidad, la minimización de datos, la exactitud de los datos, la confidencialidad, licitud de tratamiento, el consentimiento, el consentimiento del menor, las categorías especiales de datos, el tratamiento de los datos de naturaleza penal, el tratamiento de los datos sin identificación y otros como el principio de periodos de conservación limitados, el principio de la calidad de los datos, el principio de la protección de los datos desde el diseño y por defecto y el principio de las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes, artículo 4, Normas corporativas vinculantes, Reglamento (EU) 2016/679).

b. El DPO deberá estar al documento "Ejerce tus derechos" y en conjunción con el documento de la AEPD de noviembre de 2019 denominado "Guía para pacientes y usuarios de la Sanidad". Además vigilará los derechos que proclaman el Capítulo III del Reglamento (UE) 2016/679 y el Título III de la Ley Orgánica 3/2018 son los que se describen a continuación: La transparencia e información al afectado; el derecho de acceso: el derecho a la rectificación, el derecho a la supresión, el derecho a la limitación del tratamiento, el derecho a la portabilidad, el derecho de oposición, derecho a presentar una reclamación ante una autoridad de control, el derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento, representación de los interesados, derecho a indemnización y responsabilidad. Además de resolver las reclamaciones que interpongan las personas legitimadas, en base al artículo 37 de la Ley Orgánica 3/2018.

4. El régimen del nombramiento de delegado de protección de datos:

   a. Puede ser designación voluntaria u obligatoria

   b. Obligado:

      1) Con carácter general:

         artículo 37.1.b) RGPD: las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala

      2) Sector público:

         Artículo 37.1. a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial

         Artículo 37.3 RGPD Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar

un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

3) En el sector sanitario público y privado:

Artículo 37.1c) RGPD: las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 34.1.L) de la Ley Orgánica 3/2018: Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual

c. Infracciones por incumplimiento: La no designación de delegado de protección de datos es una infracción considerada grave por el artículo 73.V) Ley Orgánica 3/2018.

13º. Se confirma la existencia de disfuncionalidades en la aplicación del Reglamento (UE) 2016/679 en el ámbito de la sanidad tanto en aspectos de procedimiento entre los cuales destacan las bases jurídicas, principios, derechos, entre otros, como en aspectos organizativos básicamente en la aplicación e implantación de la fungirá del delegado de protección de datos, como garantía de su aplicación. Estas disfuncionalidades se han puesto de relieve durante el proceso de gestión de la alarma sanitaria causada por la pandemia COVID-19.

14º. Durante el trascurso de la Tesis quedan de manifiesto la existencia de estas disfuncionalidades en el caso de la sanidad pública Comunidad de Madrid, como ejemplo de sector sanitario público dentro de España.

15º. Un modelo de aplicación para la designación de un delegado de protección de datos en la sanidad pública.

Índice bibliográfico. Bibliografía utilizada para la elaboración de la Tesis, citas y consultas con señalamiento de página

Libros, artículos y tesis doctorales Página/s

1. Aguayo Albasini, JL. et al "Sobre la importancia del informe de alta hospitalaria". Revista Cirugía Española, 92(8), 574-576. 272

2. Aguilar Cavallo, G. (2010) "Derechos fundamentales-derechos humanos. ¿Una distinción válida en el siglo XXI?. Boletín Mexicano de derecho comparado, 43 (127), 15-70. 68

3. Aguilera Guzmán, M. et al. (2002) "Atención primaria en el INSALUD: diecisiete años de experiencia" Subdirección general de Coordinación Administradita. Instituto Nacional de la Salud. Disponible en https://ingesa.sanidad.gob.es/eu/bibliotecaPublicaciones/publicaciones/internet/docs/ap17.pdf (30/04/2021). 289

4. Alegre Ávila, JM. y Sánchez Lamelas, A. (2020) "Nota en relación a la crisis sanitaria generada por la actual emergencia vírica". Asociación española de profesores de derecho administrativo. Disponible en http://www.aepda.es/AEPDAEntrada-2741-Nota-en-relacion-a-la-crisis-sanitaria-generada- por-la-actual-emergencia-virica.aspx (28/02/2021). 384

5. Alexy, R. (1993) "Teoría de los Derechos Fundamentales". Ed. Centro de Estudios Políticos y Constitucionales, Madrid, Madrid, 1ª edición. 77

6. Altmann DM, et al. (2020) "What policy makers need to know about COVID-19 protective immunity". Lancet, 395. https://doi.org/10.1016/S0140-6736(20)30985-5 (28/02/2021). 396

7. Angier, N. (13 septiembre 2000) "La genética descalifica el concepto de raza". EL PAIS. Disponible en https://elpais.com/diario/2000/09/13/futuro/968796001_850215.html (28/02/2021). 52

8. Arroyo Jiménez, L. (2009), "Ponderación, proporcionalidad y Derecho administrativo" InDret. Revista para el análisis del derecho, 2, 2-32. 88, 89

9. Auby, JB. (2018) "Algorithmes et Smart Cities: Données Juridiques", Revue Générale du Droit, 2018, pp. 3-4 ; 15-18 ; Contrôle de la puissance publique et gouvernance par algorithme, Galetta, D-U y Jacques Ziller, J. (Ed.) Le droit public au défi des technologies de l'information et de la communication, au-delà de la protection des donnés, Nomos. 93

10. Banacloche Palao, J. (2018), "El desarrollo de los derechos fundamentales por el poder legislativo, el poder judicial y el tribunal constitucional" Estudios de Deusto. Universidad de Deusto. 66 (2). 17-46. 88

11. Baquerizo Minuche, J. (2009) "Colisión de los Derechos Fundamentales y juicio de ponderación". Disponible en https://www.revistajuridicaonline.com/wp-content/uploads/2009/07/1-colision-derechos.pdf (28/02/2021). 78, 87, 89, 91

12. Bastida, FJ, et al (2004), "Teoría general de los derechos fundamentales en la Constitución Española de 1978". Madrid. Editorial Tecnos. 85, 88

13. Beltrán Aguirre, JL (2018) "Reglamento general de protección de datos: novedades. Adaptación de la normativa española: El proyecto de LOPD". Revista Derecho y Salud, 28 (1), p 74-76. 99, 267, 300, 333

14. Berrocal Lanzarot, AI (2011) "La protección de datos relativos a la salud y la historia clínica en la normativa española y europea". Revista de la Escuela de Medicina Legal, 18, 12-44. 297

15. Berrocal Lanzarot, AI. (2019) "Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales". Colección de derecho de las nuevas tecnologías. Madrid. Editorial Reus. 320

16. Bestard Perelló, JJ. (2016) "De lo público a lo privado y viceversa". Madrid, www.amazon.es. 49

17. Bestard Perelló, JJ. (2015) "La asistencia sanitaria pública". Madrid. Ed. Diaz de los Santos. 255, 257

18. Bordills i Rovira, F. Chavania Diaz, M. (2004), "Almacenamiento y transmisión de imágenes. PACS" Monográfico: Radiología Digital. Revista de la sociedad Española de Informática de la Salud, 45, 54-58. 39

19. Botella Pamies, E. (2019) "Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos" en Arenas Ramiro, M. (dir.), Ortega Giménez, A.(dir.), "Protección de datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)". Editorial Sepin. 236

20. Buttarelli, G. (2016) "The EU GDPR as a clarion call for a new global digital gold standard". International Data Privacy Law, 2016, 6 (2). 201

21. Breton RJL. (1983) "Las etnias". Ed. Oikos-Tau. 57

22. Burningham, D., Bennett, P., Cave. M., Herbert, D., Higham, D. (1988), "Economía". Madrid. Ediciones Piramide. 25

23. Cabra Apalategui, JM. (12 de diciembre 2016) "¿Antinomias constitucionales? Una concepción coherentista de las normas de derecho fundamental". En Encuentro en la Universidad de Oviedo con la Universidad Autónoma de México "Derechos y obligaciones en el Estado de Derecho" de 12 a 15 de diciembre. 87

24. Cann, RL.; Stoneking, M., Wilson, AC. (1987) "Mitochondrial DNA and human evolution". Nature, International journal of science, 325, 31-36. 52

25. Cordones, A. (2002) "Protección de datos de carácter personal en la oficina de farmacia". OFFARM, 21 (1), 112-117. Disponible en https://www.elsevier.es/es-revista-offarm-4-articulo-proteccion-datos-caracter-personal-oficina-13025054. (30/04/2021). 375

26. Corman, V.M. et al. (2020) "Detection of 2019 novel coronavirus (2019-nCoV) by real-time RT-PCR". Eurosurveillance: Revista europea sobre vigilancia de enfermedades infecciosas, epidemiología, prevención y control, 25 (3), 23-30. Disponible en doi: 10.2807 / 1560-7917.ES.2020.25.3.2000045 (28/02/2021). 391

27. Cortina Ll. (2015) "Sistemas de Gestión de Bases de Datos Documentales Características Principales y Metodología de diseño". Barcelona. Universitat Pompeu Fabra. 34

28. Cristea Uivaru, LN. (2017) "La protección de datos de carácter sensible en el ámbito europeo. Historia clínica digital y big data en salud". Tesis Doctoral. Facultad de Derecho, Universidad Abad Oliva, CEU, Barcelona, España. 152

29. Cruz Villalón, P. (1984) "Estados excepcionales y suspensión de garantías". Madrid. Edi. Tecnos. 384

30. Cruz Villalon, P. (1989) "Formación y evolución de los derechos Fundamentales". Revista Española de Derecho Constitucional, 29, 35-62. 67, 68

31. Curiel Herrero, J.; Estévez Lucas, J. (2003) "Manual para la gestión sanitaria y de la historia clínica hospitalaria". Madrid. Ed. Editores Médicos. 328

32. Damián Moreno, J. (2016) "Lección. Tener o no tener legitimación. De eso se trata". Derecho procesal. Disponible en www.almacendelderecho.org. (28/02/2021). 146

33. De Esteban, J.; Gonzalez-Trevijano, J. (1992) "Curso de Derecho Constitucional Español I". Madrid. Servicios de publicaciones facultad derecho Universidad Complutense de Madrid. Reimpresión 1994. 67, 69 (2), 70

34. De la Sierra, S., (2020), "Lectura de urgencia de las reacciones frente al COVID-19 desde la óptica jurídica internacional comparada". El Cronista del Estado Social y Democrático de Derecho, 86-86; 32-41. 91

35. Diez-Picazo L., Gullón A. (1997), "Sistema de derecho civil. Volumen I". Madrid. Editorial Tecnos. 9ª edición revisada. 87

36. Drougkas, A.; Liveri, D.; Zisi, A. Kyranoudi P. (febrero de 2020) "Cloud security for Healthcare sercices". European Unión Agency Cibersecurity. Disponible en https://www.enisa.europa.eu/ publications/ report-files/translation-procurement-guidelines-for-cybersecurity-in-hospitals/ procurement-guidelines-full-version-es.pdf. (30/04/2021). 214

37. Elvira Perales, A. (2006), "Sinopsis artículo 18 de la Constitución Española". Congreso de los Diputados. Portal temático. Disponible en http://www.congreso.es/consti/ constitucion/indice/ sinopsis/sinopsis.jsp?art= 18&tipo=2 (28/02/2021). 76

38. España M. (2019) "Entrevista en Revista Registradores de España". Revista del Consejo General de Colegios de Administradores de Fincas -CGCAFE-, 84 ,20-23 Disponible en https://afcolegiadosblog.com/2019/07/30/entrevista-mar-espana-directora-de- la-agencia-espanola-de-proteccion-de-datos/ (28/02/2021). 95

39. Espuny Vidal, MC. (2003), "La aplicación del derecho". A parte rei. Revista de filosofía del derecho, 25, 1-7. 87

40. Esteve Pardo, J. (2020) "La apelación a la ciencia en el Gobierno y gestión de la crisis COVID-19", Revista de Derecho Público: Teoría y Método, 2, 35-50. https://repositorio.uam.es/handle/10486/692224. (30/04/2021). 92, 385

41. Fernández de Gatta Sánchez, D. (2020) "El Estado de Alarma y las medidas contra el coronavirus ante jueces y tribunales", Diario La Ley, 9651. Disponible en https://diariolaley.laleynext.es/dll /2020/06/17/el-estado-de-alarma-y- las-medidas-contra-el-coronavirus- ante-jueces-y-tribunales (28/02/2021). 384

42. Fernández Jara, M, (16 abril 2020) "UGT exige test de detección de Covid-19 para el personal de supermercados". Europa Express. Disponible en https://www.europapress.es/cantabria/noticia-ugt-exige-test-deteccion-covid-19-personal- supermercados-20200416135425.html (30/04/2021). 393

43. Fernández Rodríguez, JJ., (2018) "Aproximación general a la reforma normativa: el Reglamento Europeo. Principios Generales", en CAMPOS ACUÑA, C. (Dir.), Aplicación 173

Práctica y Adaptación de la Protección de Datos en el Ámbito Local. Novedades tras el Reglamento Europeo. Madrid, Ed.Wolters Kluwer.

44. Ferrón Vidán, L. (2014) "Mapa de riesgo químico". ISSGA. Instituto Gallego de Seguridad y Salud Laboral Sector Industrial. Xunta de Galicia. Santiago de Compostela. Disponible en http://issga.xunta.gal/export/sites/default/recursos/descargas/documentacion/publicacions/MRQ_CAS_20140604_DEF_WEB.pdf (31/01/2021). 222

45. Freire Campo, JM. (2007) "Los sistemas de aseguramiento sanitario de riesgos de enfermedad en España". Extraordinario Foro SESPAS-AJS. 5 (2), 41-59. Disponible en file:///C:/Users/Juan%20J/Downloads/Dialnet-LosSistemas DeAseguramientoSanitarioDeRiesgosDeEnfe-2349374.pdf (31/01/2021). 285

46. Gallego Riestra, S. (2016) "Los derechos de acceso, rectificación, cancelación y oposición del paciente sobre su historia clínica". Revista Derecho y salud, 26 (1), 133-140. 332, 334, 339

47. Gamero Casado, E. (7 noviembre 2019) "Criterios determinantes de la forma de gestión de los servicios públicos; especial referencia a la remunicipalización de servicios locales". La Administración al día. Instituto Nacional de Administración Pública. Disponible en http://laadministracionaldia.inap.es/noticia.asp?id=1510094 (31/01/2021). 424

48. García Garrido S. (2003) "Organización y gestión integral del mantenimiento". Madrid. Ed. Diaz de Santos. 333

49. García Gómez MM. (1994) "Los mapas de riesgos. Concepto y metodología para su elaboración" Rev. San.Hig. Pub, 68 (4), 443-453. 221

50. García Gonzalo R. (2 de julio de 2028). "Mecanismos de Coherencia". AEPD-UIMP, Santander 2 de julio de 2018. 243

51. García-León, FJ. et Al (2029) "La evaluación de impacto en protección de datos en los proyectos de investigación". Gaceta Sanitaria. 2020; 34(5): 521–523 Disponible en https://reader.elsevier.com/reader/sd/pii/S0213911119302675?token= C5CE040986C46130913021C379F1DFAC33A700468EA3029465A130FC1C 8A4B8B0BC92C4A523EAA799B4BC5AB51E9F35B. (28/02/2021). 218

52. García Pérez, RM. (2020) "Bases jurídicas relevantes del tratamiento de datos personales en la contratación de contenidos y servicios digitales" Cuadernos de Derecho Transnacional. Marzo 2020. Vol. 12, Nº 1, pps. 875-907. 149

53. Garrido Falla, F. (1992) "Tratado de Derecho Administrativo. Volumen II". Edición 10ª. Madrid. Ed, Tecnos. 424

54. Garrizosa Prieto, E. (2004), "El principio de proporcionalidad como mecanismo de control de las injerencias en el derecho de huelga". Revista andaluza de trabajo y bienestar social, 77, 83-123. 84

55. Gascón Marcén, A. (2020) "La regulación del flujo de los datos personales entre la Union Europea y el Reino Unido tras el Brexit". Cuadernos de Derecho Transnacional, 12 (1), 231-246. 187

56. Gasulla, A. (2018) "El Reglamento Europeo de Protección de Datos y las oficinas de farmacia". Aula Farmacia. Disponible en http://www.auladelafarmacia.com/articulo/gestion/reglamento-europeo-proteccion- datos-oficinas-farmacia/ 2018 1112 111247002519.html. (30/04/2021). 415, 417

57. Gavara de Cara, JC. (1994) "Derechos fundamentales y desarrollo legislativo. La garantía del contenido esencial de los derechos fundamentales en la Ley Fundamental de Bonn". Tesis doctoral. Universidad Autónoma de Barcelona. De 1 enero de 1994. Barcelona. España. Disponible en http://www.cepc.gob.es/Controls/ Mav/getData.ashx?MAVqs=~aWQ9MzU1MzkmaWRlPTEwMzcmdXJs PTE1Jm5hbWU 9UkNFQ18xOV8yMDkucGRmJmZpbGU9UkN FQ18xOV8yMDkucGRmJnRhYmxhPUF ydGljdWxvJmNvbnRlbn Q9YXBwbGljYXRpb24vcGRm. (28/02/2021). 69

58. Gavidia, V. Talavera M. (2012) "La construcción del concepto de salud". Didáctica de las ciencias experimentales y sociales,26, 161-175. 254

59. Gil, T. (22 abril 2020). "Medidas contra el coronavirus: qué es el "pasaporte o carné de inmunidad" a la covid-19 y por qué genera polémica". BBC News. Disponible en https://www.bbc.com/mundo/noticias-52377212. (31/05/2020). 394, 395

60. Gil Flores, J. (1994) "Análisis de datos cualitativos. Aplicación a la investigación cualitativa". Barcelona. Edit. PPU. 1994. Cap 1. Universidad de Murcia. Disponible en www.um.es/docencia/pguardio/documentos/Tec3.pdf. (31/01/2021). 25

61. Gil Membrado, C. (2011) "La e-receta: confidencialidad y proyecto de regulación". Revista derecho y salud, 21 (1), 31-60. 353, 354

62. Gómara Hernández, J.L. (2018) "Protección de Datos: el RGPD en las Entidades Locales", Barcelona, Ediciones Lefebvre. 171

63. Gómez García, P. (1998) "Las ilusiones de la identidad. La etnia como seudoconcepto". Gazeta de Antropología", 14, 13-15. 57

64. Gómez Navajas, J. (2008) "La protección de datos personales en el Código Penal español". Revista Jurídica de Castilla y León,16, 325-372. 77

65. Gómez Piqueras, C. (2009) "Disociación/anonimización de los datos de salud". Revista Derecho y Salud, 18 (1), 43-56. 332

66. González Escudero, A. (2011), "Sinopsis artículo 18 de la Constitución Española". Congreso de los Diputados. Portal temático. Disponible en http://www.congreso.es/consti/ constitucion/indice/ sinopsis/sinopsis.jsp?art =18&tipo=2. (28/02/2021). 76

67. González Feijoo, M. (2020) "Todo lo que debes saber sobre los tests de diagnóstico de COVID-19". EnfermeríaTV. Disponible en https://enfermeriatv.es/es/el-mejor-metodo-diagnostico/ (31/01/2021). 391

68. González de la Peña, AS. (2017) "El secreto del profesional sanitario: Limitaciones y Singularidades", V Promoción Máster en Derecho Sanitario Universidad San Pablo CEU. Madrid. 263

69. Gonzalo Domenech, JJ. (2019) "Las decisiones de adecuación en el derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de aplicación por los Estados Miembros". Cuadernos de Derecho Transnacional. 11 (1), 350-371. 182, 186

70. Guasch Portas, V. (2015) "El interés legítimo en la protección de datos". Revista de Derecho UNED, 16, 417-438. 112

71. Heller, H. (1934) "Teoría del Estado" (Política Y Derecho) (Spanish Edition). Fondo de Cultura Económica. Edición de Kindle. Primera edición electrónica, 2015. 68

72. Heller, H. (1934) "Teoría del Estado" México. Ed. Fondo de cultura económica. Decimosegunda reimpresión 1987. 78

73. Herranz Ortiz, AI. (2003) "El derecho a la protección de datos en la sociedad de la información". Bilbao. Instituto de Derecho Humanos. Universidad de Deusto. 77

74. Herrero Jaén, S. (2016). "Formalización del concepto de salud a través de la lógica: impacto del lenguaje formal en las ciencias de la salud". Santa Cruz de la Palma. ENE Revista de Enfermería, 10(2). Disponible en http://scielo.isciii.es/ scielo.php?script=sci_arttext&pid=S1988-348X2016000200006 (31/01/2021). 259

75. Hesse, K. (1978) "Bestand und Bedeutung der Grundrechte in der Bundesrepublik Deutschland", en "Europäische Grundrechte-Zeitschrift" -5-, H. 19-22. Ed. N.P. Engel Verlag, Kehl am Rhein (Alemania), 1978. 78, 93

76. Hidalgo Cerezo, A. (2016) "Protección de datos de carácter personal relativos a la salud del paciente: fundamentos, protección a la intimidad y comentarios al Reglamento UE 2016/679". Revista de Derecho UNED, 19, 715-744. Disponible en http://revistas.uned.es/index.php/ RDUNED/ article/ viewFile/ 18462/15501 (28/02/2021). 269, 311

77. Hidalgo Vela, A.; Corugedo de las Cuevas, I.; del Llano Señaris, J. (2000) "Economía de la salud". Madrid. Ediciones Pirámide. 253

78. Horcajada P., Padilla, B. (2013) "Endemia y epidemia. Investigación de un brote epidémico nosocomial". Enfermedades Infecciosas y Microbiología Clínica, 31(3), 181-186. 162 (2)

79. Huerta Aragonés, J.; Cela de Julián, E. (2 febrero 2018) "Hematología práctica: interpretación del hemograma y de las pruebas de coagulación". 15º Curso de actualización en pediatría. AEPap Disponible en file:///C:/Users/Juan%20J/Documents/ TRABAJO%20DE%202021/ DOCTORADO %202018/ TRABAJOS%20SOBRE%20LA%20TESIS/ REDACCION%20DOCUMENTO/ NUEVA% 20VERSION%20TESIS/VERSIONES%20MODIFICADAS%20POR%20BLANCA/ BILBLIOGRAFIA%20TESIS/ HUERTA%2020PG.pdf (28/02/2021). 265

80. Ibáñez Martí, C. (27 febrero 2007) "Qué es un brote epidémico". Fundación para el conocimiento Madrid. Blog. Disponible en http://www.madrimasd.org/blogs/salud_ publica /2007/02/28/ 60163 (31/05/2020). 161

81. Iturralde Sesma, V. (1999) "Sobre el concepto de jerarquía normativa". Anales de la Cátedra Francisco Suárez, 33, 261-277. 82

82. Jorro, I. (19 abril 2020) "Torra y Mitjà proponen clasificar a los ciudadanos y seguirles por el móvil". Crónica global. Disponible en https://cronicaglobal.elespanol.com/ politica/torra-oriol-mitja-codigo-colores_339648_102.html (31/01/2021). 394

83. Kelsen, H. (1960) "Teoría pura del Derecho". Buenos Aires. Editorial Universitaria de Buenos Aires. 4º Ed. 9ª reedición, 2009. 82

84. Koontz, H., Weihrich. H. (1990) "Administración". México. Ed. McGraw-Hill. 27

85. Lalonde, M. (1974) "A new perspective on the health of Canadians". A working document. Otawa. 255

86. Lalonde, M. (2002) "A new perspective on the health of Canadians: 28 years later". Rev Panam Salud Públic, 12 (3), 149-152. 255

87. Lazpira Gurtuban, M. (1994) "Análisis comparado de las Legislaciones sobre Protección de Datos de la Estados miembros de la Comunidad Europea". Revista Informática y Derecho, 6 y 7, 397-420. 24, 26, 225

88. Loeffelholz, MJ.; Tang, Yi-Wei (2020) "Laboratory diagnosis of emerging human coronavirus infections – the state of the art". Emerging Microbes & Infections. 9 (1), 747-756, Disponible en https://doi.org/10.1080/22221751.2020.1745095 (28/02/2021). 392

89. López Álvarez, LF. (2017) "Protección de datos personales: adaptaciones necesarias al nuevo Reglamento Europeo". Madrid. Ed. Lefebvre. 171

90. López Garrido, L. (2018) "La protección de datos personales y el caso Facebook: una cuestión trasnacional". Revista Privacidad y Derecho Digital, 11, 147-173 Año III. 150

91. López-Picazo Ferrer, J.J. et Al (2002) "Datos clínicos esenciales de la historia clínica de atención primaria: una experiencia de evaluación y mejora". Atención primaria, 30 (2), 92-98. 323

92. López González, R. (19-21 noviembre de 2008) "CMBD ¿Qué es y para qué nos sirve?." XXI Congreso Nacional de la SEMI. Disponible en https://www.fesemi.org/sites/default/files/ documentos/ ponencias/ xxix-congreso-semi/Dr.%20Lopez%20GOnzalez.pdf (31/05/2021). 294

93. Llaneza González, P. (2018) "Nuevo maco de cumplimiento en las obligaciones de protección de datos: la gestión de la privacidad desde la mitigación del Riesgo". Revista Privacidad y Derecho Digital, 11, 77-107, Año III. 205

94. Mandado Pérez, E.; Mandado Rodríguez, Y. (2015) "Sistemas electrónicos digitales". Marcombo ediciones técnicas. 10ª Edición. 38

95. Marco Cuenca, G.; Salvador Olivan, J.A. (2018) "Del CMBD al Big Data en salud: un sistema de información hospitalaria para el siglo XXI". Scire: representación y organización del conocimiento, 24 (1), 77-89. 294

96. Marcos Fernández, A. et al (2018) "Fundamentos del Derecho Administrativo". Madrid. Servicio de Publicaciones de la Universidad Autónoma de Madrid. 83

97. Marcos, T. (2018) "Renovando la satisfacción del cliente". Revista de la normalización española. Disponible en https://revista.une.org/ 2/renovando-la-satisfaccion-del-cliente.html (31/05/2021). 239

98. Marmot M., Wilkinson RG. (2013) "The solid facts". Copenhagen. WHO Regional Office for Europa. Disponible en https://www.euro.who.int/ data/ assets/ pdf_file/ 0005/ 98438/ e81384.pdf. (28/02/2021). 255

99. Marqués Racionero, MJ. et al. (2012) "Guía de elaboración de mapa de riesgos" EnfermNefrol, 15(1), 176-177. 222

100. Marshall, A. (1890) "Principles of Economics: an introductory text". Reimprison 2013. 25

101. Martínez Ascetas, R., (2007) "El derecho fundamental a la protección de datos: perspectivas", Revista d'Internet, Dret i Politica, 5, 47-61. 75

102. Martínez Martínez, R., (2020) "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", Diario La Ley, 9601. 91

103. Mauzo, J. (25 abril 2020) "La OMS rechaza el pasaporte inmunitario por falta de evidencia sobre el riesgo de segundas infecciones". El País. Disponible en 395

https://elpais.com/sociedad/2020-04-25/la-oms-rechaza-el- pasaporte-inmunitario-por-falta-de-evidencia-sobre-el-riesgo-de-segundas- infecciones.html (28/02/2021)

104. Mediavilla, J. (7 febrero 2016) "¿Debemos seguir empleando el concepto de raza?" EL PAIS Disponible en https://elpais.com/elpais/2016/02/05/ciencia/ 1454696080_059342.html (28/02/2021). 52

105. Mediavilla, J, (7 abril 2020) "Coronavirus España: nace el primer carnet de inmunidad al Covid-19". Redacción médica. Disponible en https://www.redaccionmedica.com/autonomias/ castilla-leon/coronavirus-espana-nace-el-primer-carnet-de-inmunidad- al-covid-19-4009 (31/05/2020). 394

106. Medina Guerrero, M. (1996) "La vinculación negativa del legislador a los derechos fundamentales". Madrid, McGraw-Hill Interamericana de España. 85

107. Medinaceli Díaz, KI. (2016) "El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano", Tesis Doctoral. Facultad de Ciencias de la Educación, Universidad Pontificia Comillas. Madrid. España. 151, 152, 159, 268, 285

108. Menéndez Rexach, A. (2003) "Ley y Reglamento en España", en Rosado Pacheco, S. (coord..): Derecho Europeo Comparado sobre Ley y Reglamento, pps 93-210, Madrid, Centro de Estudios Ramón Areces. 81

109. Merino Norverto, M. (2003) "Sinopsis artículo 10 de la Constitución Española" Congreso de los Diputados. Portal temático. Disponible en https://app.congreso.es/consti/constitucion/indice/ sinopsis/ sinopsis.jsp?art =10&tipo=2 (28/02/2021). 54

110. Miralles López, R. (2017) "Desvinculando datos personales: seudonimización, desidentificación y anonimización". Revista de la Sociedad Española de Informática y Salud, 122. 335

111. Monereo Atienza, C. (2 julio 2014) "Aproximación conceptual a la orientación sexual e identidad de género: estrategias político-jurídicas para la reivindicación de derechos del colectivo LGBT" Comunicación Congreso Universitario Internacional Investigación y Género (5º). Sevilla. Disponible en https://idus.us.es/bitstream/ handle/ 11441/41135/ Pages%20from% 20Investigacion_Genero_14-2-5.pdf? sequence= 1&isAllowed=y. (31/01/2021). 58

112. Monereo Pérez, JL.; Fernández Avilés, JA. (2008) "La libertad sindical en la doctrina del Tribunal Constitucional", Revista del Ministerio de Trabajo y Asuntos Sociales, 73, 247-312. 51

113. Montserrat Sánchez-Escribano, MI. (2015) "Libertad informativa y protección de datos: desarrollo de la jurisprudencia del Tribunal Constitucional y tutela penal en el delito de descubrimiento y revelación de secretos". Anuario Iberoamericano de Justicia Constitucional, 19, 323-363. 76

114. Moreno Zambrano, V. (2019) "Minería de datos en plataformas de entretenimiento de cara al RGPD". Revista Privacidad y Derecho Digital, 13, 157-168. Año III. 27

115. Murillo de la Cueva, PL. (1999) "La construcción del derecho a la autodeterminación informativa". Revista de Estudios Políticos (Nueva Época), 104, 35-60. 28

116. Navarro Ruiz, G. (2019) "Aplicación de la tecnología blockchain a emisiones de valores negociables". Revista Privacidad y Derecho Digital, 15, 127-170. Año IV. 27

117. Olmedilla Zafra, A., Carmen García Montalvo, C., Martínez Sánchez, F. (2006) "Factores psicológicos y vulnerabilidad a las lesiones deportivas: un estudio en Futbolistas". Revista de Psicología del Deporte (Universitat de les Illes Balears. Universitat Autónoma de Barcelona) Vol. 15 (1), 37-52. 213

118. Ortega Klein, A. (12 mayo 2020) "La búsqueda de inmunidad digital frente a la pandemia: eficacia, privacidad y vigilancia". Documento de trabajo 9/2020 - 12 de mayo de 2020 - Real Instituto Elcano. p 20. 114

119. Ortiz López, P. (2018) "Los datos personales. ¿Una propiedad o un derecho fundamental?". Revista Privacidad y Derecho Digital, 10, 179-182. Año III. 28

120. Pascua Mateo, FA. (2019) "Un nuevo capítulo en la tutela del derecho a la protección de datos personales: los datos de contenido político". Comentario a la Sentencia del Tribunal Constitucional 76/2019, de 29 de mayo, en el recurso de inconstitucionalidad núm. 1405-2019 (BOE núm.151, 25 de junio de 2019", Revista de las Cortes Generales, 106, 549-558. 74

121. Pascual Huerta, P. (2017) "La génesis del derecho fundamental a la protección de datos Personales", Tesis Doctoral, Facultad de Derecho, Universidad Complutense de Madrid. Madrid. España. 104

122. Peces-Barba, G. "Derechos Fundamentales" Disponible en https://e-archivo. uc3m.es / bitstream/ handle/ 10016/10462/derechos_Peces;jsessionid= A8CC67612F2D8A33739CDC759A2E49E5?sequence=1 (28/02/2021). 69

123. Peces-Barba, G. et Al (1999) "Curso de teoría del derecho". Disponible en https://e-archivo.uc3m.es/bitstream/handle/10016/ Madrid. Editorial Marcial Pons. 87

124. Pérez Luño, AE. (1984) "Los derechos fundamentales". Editorial Tecnos. ebook edición Kindle de 2013. 78

125. Picard, M. (2014) "Leyes y reglamentos eficaces para la reducción del riesgo de desastres: Informe multinacional". PNUD. Naciones Unidas. ONU. Federación internacional de sociedades de la Cruz Roja y de la Media Luna Roja. Disponible en https://www.undp.org/content/dam/undp/library/crisis%20prevention/UNDP_CPR _ DRRLaw_Spanish_Aug2014.pdf (31/01/2021). 222

126. Pino, G. (2009) "Conflictos entre derechos fundamentales. Una crítica a Luigi Ferrajoli". DOXA, Cuadernos de Filosofía del Derecho, 32, 647-664. 78

127. Pita Fernández, S.; Pértega Díaz, S. (2001) "Estadística descriptiva de los datos", Atención primaria en la red. 8: 37-41. 24

128. Polo Roca, A., (2019) "Protección de datos y elaboración de perfiles: el nuevo artículo 58.bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general", Revista Galega de Administración pública (REGAP), 58, 507-527. 80

129. Pozzi, S. (12 julio 2019) "EE UU multa a Facebook con 5.000 millones por violar la privacidad de los usuarios". El País. Disponible en https://elpais.com/economia/2019/07/12/ actualidad /1562962870_283549.html (31/05/2020). 252

130. Prego de Oliver Fernández, JA. (2017) "La transparencia como elemento de apoyo al consentimiento en materia de Protección de Datos", Tesis Doctoral, Facultad de 379

Derecho, Universidad Carlos III de Madrid, Getafe, España. Disponible en https://e-archivo.uc3m.es/handle/10016/26447#preview. (30/04/2021).

131. Prieto Herguera, J. (29 junio 2016) "Códigos de Conducta, certificaciones y trasferencias internacionales" 8.ª Sesión Anual Abierta de la AEPD. Gran Auditorio Ramón y Cajal. 29 de junio de 2016. 240

132. Pulido, S. (12 de marzo de 2020) "¿Cuál es la diferencia entre brote, epidemia y pandemia?". Gaceta sanitaria. Disponible en https://gacetamedica.com/investigacion/ cual-es-la-diferencia-entre-brote-epidemia-y-pandemia/ (28/02/2021). 162 (2)

133. Puyol Montero, J. (2016) "Los principios del derecho a la protección de datos", en PIÑAR MAÑAS, J.L. (Dir.) Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad, Reus. 171

134. Quadra Salcedo, T.; Piñar Mañas, JL.; M. Barrio, A.; Torregrosa Vázquez, J. (2018) "Sociedad digital y derecho". Ministerio de Industria, Comercio y Turismo. Madrid. Boletín Oficial del estado. 25

135. Quesada Monge, DF. (2017) "Transparencia administrativa, acceso a la información y protección de datos personales: criterios para una conciliación de derechos desde la jurisprudencia del TJUE y la Ley 19/2013, de 9 de noviembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno". Tesis Doctoral. Faculta de Derecho. Universidad Autónoma de Madrid. Madrid. España. 120

136. Rallo Lombarte, A. "El nuevo derecho de protección de datos", en "Revista española de derecho constitucional", año Nº 39, Nº 116. Ed. Centro de Estudios Políticos y Constitucionales, Madrid, 2019. 73

137. Requejo Naveros, MT. (2007) "El secreto profesional del médico y su protección jurídico penal: una perspectiva histórica". Foro, Nueva Época, 6, 159-194. 152

138. Robles Garzón, JA. (2013) "Conceptos básicos de derecho procesal civil" Madrid. Editorial Tecnos, Grupo Anaya. 146 (3)

139. Rodríguez de Santiago, JM. (2000) "La ponderación de bienes e intereses en el Derecho administrativo". Madrid. Marcial Pons. 85, 91

140. Rodríguez de Santiago, JM. (2007) "La Administración del Estado social". Madrid. Marcial Pons. 177

141. Rodríguez Gómez, D. (2006) "Modelos para la creación y del conocimiento: una aproximación teórica". Educar. 37, 25-39. 25

142. Rodríguez López, M. et al. (2013) "Mapa de Riesgos: Identificación y Gestión de Riesgos" Finanzas y Sistemas de Información para la Gestión (FYSIG), 2 (1), 1-29. 221

143. Rodríguez-Chaves Mimbrero, B. (2020) "Salud versus privacidad: ¿podemos conservar ambas? Unos apuntes sobre la gestión de la pandemia por covid-19 desde los ámbitos de la regulación y aplicación del derecho". En BERMÚDEZ SANCHEZ J., DE MARCOS FERNÁNDEZ A. et al en "Transparencia, lobbies y protección de Datos" Madrid, Editorial Thomson Reuters. 79, 88

144. Roger, FH. (1981) "The minimum basic data set for hospital statistics in the EEC". Commission of the European Communities. ECSC-EEC-EAEC, Brussels. Luxembourg. pp-2-3. 294

145. Rule, JB.; Greenleaf, G. (2008) "Privacy Protection: The First generation", USA. Edward Elgar. 29

146. Ruiz Miguel, C. (2003) "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico". Revista de Derecho Comunitario Europeo, 7 (14), 7-43. 65

147. Ruiz Ruiz, R. (2007) "La ponderación en la resolución de colisiones de derechos fundamentales. Especial referencia a la jurisprudencia constitucional española" Revista Telemática de Filosofía del Derecho, 10, 53-57. 71

148. Sánchez-Caro, J.; Abellán, F. (2003) "Derechos y deberes de los pacientes", Granada, Ed. Comares. 152, 340

149. Sánchez González, S (2003) "De la imponderable ponderación y otras artes del Tribunal Constitucional". La Revista Teoría y Realidad Constitucional, 12-13, 351-382. 71

150. Segura Benedicto, A. (2014) "Recortes, austeridad y salud". Gaceta Sanitaria, 28 (1), 7-11. 257

151. Segura Egea, JJ. (2002) "Sensibilidad y especificidad de los métodos diagnósticos convencionales de la caries oclusal según la evidencia científica disponible". RCOE (revista del Ilustre Consejo General de Colegios de Odontólogos y Estomatólogos de España), 7 (5), 491-501.Disponible en http://scielo.isciii.es/scielo.php?script= sci_arttext&pid=S1138-123X2002000600004 (31/05/2020). 392

152. Serrat Romani, M. (2017) "Los derechos de los contribuyentes en un entorno digital". Revista Privacidad y Derecho Digital. 7, 67-107. Año II. 23, 24

153. Sieira, S. (2011) "Sinopsis artículo 10 de la Constitución Española" Congreso de los Diputados. Portal temático. ¿Disponible en https://app.congreso.es/consti/ constitucion/indice/sinopsis/sinopsis.jsp?art= 10&tipo=2 (28/02/2021). 54

154. Siso Martín, J (18 y 19 abril 2017) "La historia clínica. Su importancia en el proceso de responsabilidad sanitaria y su valor como medio probatorio". Curso "Responsabilidad sanitaria y la nueva configuración legal de la imprudencia médica". Disponible en http://www.juansiso.es/ Almacen/ HISTORIA%20 CLINICA%20Y% 20SU%20 IMPORTANCIA %20EN% 20EL %20PROCESO %20DE %20 RESPONSABILIDAD %20 SANITARIA.pdf. (28/02/2021). 270, 326

155. Spence Michael A., Zeckhauser R. (1971) "Seguro, Información y Acción Individual". American Economic Review 61 (2), 380-387. Disponible es file:///E:/SPENCE%209PG.pdf. (30/04/2021). 253

156. Tapia Granados, J.A. (2011) "La mejora de la salud durante las crisis económicas" España Papeles de relaciones ecosociales y cambio global, 113, 121-137. 256

157. Temes, JL. (2002) "Gestión Hospitalaria". Madrid. Ed. McGraw-Hill. 294

158. Templeton, AR. (2013) "Razas biológicas en humanos". Estudios en historia y filosofía de las ciencias biológicas y biomédicas vol. 44,3. 262-71. 52

159. Theimer, S. (2020) "Falsos negativos en prueba de COVID-19 pueden llevar a errónea sensación de seguridad". Mayo Clinic News Network. Disponible en https://newsnetwork.mayoclinic.org/discussion/ falsos-negativos-en-prueba-de-covid-19-pueden-llevar-a-erronea- sensacion-de-seguridad/ (31/01/2021). 392

160. Velasco Caballero, F. (2020) "Libertad, Covid-19 y proporcionalidad (I): fundamentos para un control de constitucionalidad". Disponible en: 91

https://franciscovelascocaballeroblog.wordpress.com/2020/05/30/ libertad-covid-19-y-proporcionalidad-i- fundamentos-para-un- control-de-constitucionalidad/ (28/02/2021).

161. Velasco Caballero F. (2020) "Libertad, Covid-19 y principio de proporcionalidad (II): indicadores para el control de constitucionalidad." Blog independiente de Francisco Velasco Disponible en https://franciscovelascocaballeroblog.wordpress.com/ 2020/05/31/libertad-covid-19-y-principio-de- proporcionalidad-ii-indicadores-para-el-control-de-constitucionalidad/ (28/02/2021). 92

162. Verdú, D. (14 abril 2020) "Un carné de inmunidad es una estupidez enorme". El País. Disponible en https://elpais.com/sociedad/2020-04-14/ un-carne-de-inmunidad-es-una-estupidez-enorme.html (31/05/2020). 394

163. Vidal Gil, E. (2001) "La Interpretación de los Derechos Fundamentales por el Tribunal Constitucional". Anuari de dret parlamentari. 11, 73-112. Disponible en https://www.cortsvalencianes.es /sites/default/files/ media/file_author/73_0.pdf (28/02/2021). 71

164. Villar Aguirre, M. (2011) "Factores determinantes de la salud: Importancia de la prevención". Acta médica peruana, 28(4), 237-241. Disponible en http://www.scielo.org.pe/pdf/amp/ v28n4 /a11.pdf (28/02/2021). 255

165. Villaverde Menéndez, I. (2007) "La función de los derechos fundamentales en el marco del Estado de las Autonomías" Revista d'Estudis Economics i Federals,4, 203-239. 70

166. Villaverde Menéndez, I. (2015) "Los derechos fundamentales en la historia. Una aproximación a su origen y fundamento". En CARBONELL SANCHEZ et Al "Estado constitucional, derechos humanos, justicia y vida universitaria". Estudios en homenaje a Jorge Carpizo. Derechos humanos, tomo V, vol. 2. (573-598). 67

167. Yetano Laguna, J, López Arbeloa, G (2010) "Manual de descripción de los Grupos Relacionados por el Diagnostico". Oskidetza. Servicio Vaso de Salud. Victoria-Gasteiz. Edicón 5ª. 295

168. Żelazny, R. (2015) "Information Society and Knowledge Economy, Essence and Key Relationships". Journal of Economics and Management. Vol 20 (2), 5-22. 25

Sentencias de Tribunales españoles y TJUE (por jurisdicción y orden cronológico de más antiguo a más moderno)

Sentencias del Tribunal Constitucional (por orden cronológico) Página/s

5.	AEPD (2020). Resolución de la Agencia Española de Protección de Datos PS/00417/2019, de 9 de junio de 2020.	414, 421
6.	AEPD (2018). Resolución de la Agencia Española de Protección de Datos PS/00236/2018, de 11 de junio de 2019.	32
	Guías de la AEPD (por orden cronológico, más antiguo a más moderno)	Página/s
1.	AEPD (2004) Guía "El derecho fundamental a la protección de datos de carácter personal". Agencia Española de Protección de Datos.	75
2.	AEPD (2019) "Manual del delegado de protección de datos". Guía para los Delegados de Protección de Datos en los sectores públicos y semipúblicos sobre cómo garantizar el cumplimiento del. Reglamento General de Protección de Datos de la Unión Europea. Julio de 2019. Disponible en https://www.aepd.es/sites /default /files / 2019-12/El%20Manual%20del% 20DPD%20-%20KORFF GEORGES %20-%20ESP.pdf (31/01/2021).	226
3.	AEPD (2019) "Guía para el cumplimiento del deber de informar". Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf (28/02/2021).	106, 305
4.	AEPD (2019) "La protección de datos y la Administración Local" Guías sectoriales AEPD. Septiembre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf (31/01/2021).	399
5.	AEPD (2019) "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Madrid. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones- de-impacto-rgpd.pdf (31/01/2021).	210, 215, 216, 217, 218 (2), 219, 221, 400
6.	AEPD (2019) "Guía del Reglamento General de Protección de Datos. Para responsables del tratamiento". Guía de protección de datos UE. Septiembre 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf (31/01/2021).	95, 147, 201, 299, 423
7.	AEPD (2019) "Protección de Datos: Guía para el Ciudadano". Octubre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf (28/02/2021).	98, 99, 209
8.	AEPD (2019) "Guía de privacidad del diseño". Noviembre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf (31/01/2021).	204
9.	AEPD (2019) "Guía para pacientes y usuarios de la sanidad". Diciembre 2019. Disposición en https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf (28/02/2021).	261, 300, 304, 317, 334
10.	AEPD (2020) "Guía de protección de datos por defecto". Octubre 2020. Disponible en https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf (31/01/2021).	96, 98

Otros documentos de la AEPD (por orden cronológico, más antiguo a más moderno) Página/s

1. AEPD (2000) Memoria de la Agencia Española de Protección de Datos. 121

2. AEPD (6 Julio 2017) "Convenio de colaboración entre el Consejo General del Poder Judicial y la Agencia Española de Protección de Datos sobre colaboración en el ejercicio de las funciones propias de las autoridades de control en materia de protección de datos". Disponible en https://www.aepd.es/sites/default/files/2020-02/convenio-aepd-cgpj.pdf (28/02/2021). 193, 196

3. AEPD (2018) Grupo de trabajo sobre protección de datos del artículo 29 "Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679" Adoptadas el 3 de octubre de 2017. Revisadas por última vez y adoptadas el 6 de febrero de 2018. Disponible en https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf (31/01/2021). 209

4. AEPD (2018) "¿Qué es un delegado de protección de datos?" Diciembre 2018. Disponible en https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-un-delegado-de-proteccion-de-datos (31/01/2021). 213, 411

5. AEPD (2018) "Elaborar el registro de actividades de tratamiento". Diciembre 2018. Disponible en https://www.aepd.es/es/prensa-y-comunicacion/blog/elaborar-el-registro-de-actividades-de-tratamiento (28/02/2021). 203, 204

6. AEPD (2019) "Funciones y poderes". Enero de 2019. Disponible en https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/funcion-y-poderes. (28/02/2021). 192, 401

7. AEPD (2019) Sede Electrónica de 20 de julio de 2919. "Derecho a la limitación del tratamiento". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-limitacion-del-tratamiento (28/02/2021). 108, 308

8. AEPD (2019) Sede electrónica de 20 de julio de 2019. "Derecho de supresión ("al olvido")" Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-supresion-al-olvido (28/02/2021). 107, 307

9. AEPD (2019) Sede Electrónica de 20 de julio de 2919. "Derecho a la portabilidad". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-portabilidad (28/02/2021). 109 (2), 308 (2)

10. AEPD (2019) Sede Electrónica de 20 de julio de 2919. "Derecho a oposición". Disponible en https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-oposicion.pdf (28/02/2021). 109, 309

11. AEPD (2019) Sede electrónica de 20 de julio de 2019. "Derecho a no ser objeto de decisiones individuales automatizadas". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-no-ser-objeto-de-decisiones-individuales (28/02/2021). 103

12. AEPD (2019) Sede electrónica de 20 de julio de 2019. "Derecho de rectificación". Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-rectificacion (28/02/2021). 107, 307

13. AEPD (2019) "Ejerce tus derechos". 20 de Julio de 2019. Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos (31/01/2021). 104, 105, 304

14. AEPD (2019) "Modelo de Cláusula para contratos de encargados de tratamiento". Septiembre 2019. https://www.aepd.es/sites/default/files/2019-09/clausulas-contratos-encargado-tratamiento.pdf (31/01/2021). 207

15. AEPD (2019) "Informe del Gabinete Jurídico sobre el Interés Legítimo". Septiembre de 2019. Disponible en https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-interes-legitimo.pdf (28/02/2021). 32, 160

16. AEPD (2019) "Análisis de riesgos y adopción de medidas de seguridad". Octubre 2019. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/ medidas-de-cumplimiento/ analisis-de-riesgos (31/01/2021). 129, 207, 208

17. AEPD (2020) "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción". Febrero 2020. Disponible en https://www.aepd.es /sites/ default/files/2020-02/adecuacion-rgpd-ia.pdf (31/01/2021). 99

18. AEPD (2020) "Datos de Salud en dispositivos móviles y seguridad jurídica". La Solución DocToDoctro. Disponible en https://www.aepd.es/sites/default/files/2020-02/premio-2019-emprendimiento-Molinapps.pdf (31/01/2021). 341

19. AEPD (2020) "Medidas de protección de datos desde el diseño y por defecto" de 27 de febrero de 2020. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/proteccion-de-datos-diseno-por-defecto (28/02/2021). 205

20. AEPD (2020) "Informe sobre los tratamientos de datos en relación con el COVID-19". Gabinete Jurídico. Marzo 2020. Disponible en https://www.aepd.es/es/ documento/ 2020-0017.pdf (31/05/2020). 382

21. AEPD (2020) "Delegado de protección de datos". Junio 2020. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos. (31/01/2021). 226, 229

22. AEPD (2020) Sede electrónica de 27 de noviembre de 2020. "Códigos de Conducta". Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta (28/02/2021). 238

23. AEPD (2020) "Información sobre consentimiento para tratar datos personales de menores de edad". Diciembre de 2020. Disponible en https://www.aepd.es/sites/ default/files/2020-12/infografia-consentimiento-menores.pdf (31/01/2021). 100

24. AEPD (2021) "Transferencias internacionales". Enero 2021. https://www.aepd.es/es/ derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales (31/01/2021). 245, 247

25. AEPD (2021) "Formulario de Consulta Previa". Disponible en https://sedeagpd.gob.es/ sede-electronica-web/vistas/formConsultaPrevia/ procedimientoConsultasPrevias.jsf. (31/01/2021) 222, 400

26. AEPD (2021) "Consulta DPD" Disponible en https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf (30/04/2021). 421, 449

27. AEPD (2021) "Persona delegada en protección de datos". 30 de marzo de 2021. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/persona-delegada-en-proteccion-de (30/04/2021). 411

Índice de otras fuentes con señalamiento de página

12. MS. Ministerio de Sanidad (2020). "Historia clínica Digital del Sistema Nacional de Salud". Web del Ministerio de Sanidad. Disponible en https://www.mscbs.gob.es/ ciudadanos/portada/preguntas_frecuentes.htm (31/01/2021). 275

13. MS. Ministerio de Sanidad (2021). "Institutos de Investigación sanitaria acreditados según comunidad autónoma". Disponible en https://www.mscbs.gob.es/ estadEstudios/ sanidadDatos/ tablas/ tabla29_2.htm (31/01/2021). 447

14. MTMAU. Ministerio de transporte, movilidad y agenda urbana. "Elaboración de tarjetas de identificación y control con soporte de firma digital". Disponible en https://www.mitma.gob.es/el-ministerio/buen-gobierno/proteccion-datos-personales/rat/elaboracion-de-tarjetas-de-identificacion-y-control-con-soporte-de-firma-digital (31/01/2021). 284

15. MUFACE (2020). Mutualidad General de Funcionarios Civiles del Estado. Año 2020. Disponible en https://www.muface.es/muface_Home/muface_Index.html (31/05/2020). 273

16. MUGEJU (2020). Entidad Gestora del Régimen Especial de Seguridad Social del personal al servicio de la Administración de Justicia. Año 2020. Disponible en https://www.mugeju.es/que-es-mugeju (31/05/2020). 273

17. ONS (2018). "Normas de la Autoridad Nacional para la Protección de la Información Clasificada" Autoridad delegada para la seguridad de la información clasificada. Cuarta edición. NIPO: 083-19-040-0 (edición en línea) Disponible en https://www.cni.es/comun/recursos/descargas/ DOCUMENTO_5_-_Normas_de_la_Autoridad.pdf (28/02/2021). 198

18. UNE (2020) "Nuestra Historia ". Asociación Española de Normalización. Disponible en https://www.une.org/la-asociacion/historia (31/05/2020). 36

Documentos de Administración pública de las Comunidades Autónomas (por orden cronológico, más antiguo a más moderno) Página/s

1. SERGAS. Consejería de Saude (2015) "Sistema de Seguridad del Paciente y Gestión de Riesgos Sanitarios". Servicio Gallego de Salud. Xunta de Galicia. Disponible en https://www.sergas.es/Calidade-e-seguridade-do-paciente/ Documents/6/ SISTEMA%20 SEGURIDAD%20DEL% 20PACIENTE%20Y%20GESTION%20 DE%20REISGOS-SERGAS_castellano.pdf. 222

2. Consejería de Sanidad. Madrid (2019) "Memoria de 2019 del Servicio Madrileño de Salud". Disponible en https://www.comunidad.madrid/servicios/salud/ memorias-e-informes-servicio-madrileno-salud (28/02/2021). 446

3. SERGAS (2020) "Estudios seleccionados sobre SARS-CoV-2 y COVID-19". Consejería de Saude. Disponible en https://coronavirus.sergas.gal/Contidos/Documents/216/ Seguimiento_Publicacions_COVID19_08052020.pdf (31/01/2021). 396

4. Consejería de Sanidad. Madrid (2021) "Hospitales de la red del Servicio Madrileño de Salud". Disponible en https://www.comunidad.madrid/servicios/ salud/hospitales-red-servicio-madrileno-salud (31/05/2021). 446

5. Consejería de Sanidad. Madrid (2021) "La Gerencia de Atención primaria". Disponible en https://www.comunidad.madrid/servicios/ salud/atencion-primaria (31/05/2021). 444, 445

6. Consejería de Sanidad. Madrid (2020) "Historia clínica Digital del Sistema Nacional de Salud". Disponible en https://www.comunidad.madrid/servicios/ salud/historia-clinica-digital-sistema-nacional-salud (31/05/2020). 275

7. Consejería de Sanidad. Madrid (2021) "Portal estadístico de personal del Servicio Madrileño de Salud". Disponible en https://www.comunidad.madrid/servicios/ salud/portal-estadistico-personal-servicio-madrileno-salud (31/05/2021). 444

8. Consejería de Sanidad. Madrid (2020) "Procedimiento de detección del nuevo coronavirus SARS-CoV-2 en la Comunidad de Madrid". Dirección General de Salud Pública. Red de Vigilancia Epidemiológica. Disponible en https://www.comunidad.madrid/ sites/default/ files/doc/sanidad/epid / procedimiento_de_deteccion_del_nuevo_coronavirus_sars-cov-2_en_cm.pdf (31/05/2020). 391

9. SACYL (2021) "Dieta mediterránea" Portal de salud. Consejería de Salud de Castilla y León. Disponible en https://www.saludcastillayleon.es/es/enfermedades-problemas-salud/enfermedad-cardiovascular/prevencion-habitos-vida-saludables/dieta-mediterranea (28/02/2021). 262

Documentos de la Unión Europea (por orden alfabético) Página/s

1. ADFUE (2018) "Manual de legislación europea en protección de datos". Luxemburgo: Oficina de Publicaciones de la Unión Europea. Disponible en https://op.europa.eu/es/publication-detail/-/publication/ af9d0b3f-82be-11e5-b8b7-01aa75ed71a1/language-es (28/02/2021). 74

2. Consejo de Europa (1981) "Convenio 108 del Consejo de Europa, de 28-1-1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España el 27 de enero de 1984 (entró en vigor de forma general el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo). (BOE núm. 274 de 15-11-1985). Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447 (31/05/2020). 24

3. Comisión Europea (2010). Decisión de la comisión, 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010D0087&from=ES (28/02/2021). 180

4. Comisión Europea (2014) "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". Adoptadas el 9 de abril de 2014. Grupo de trabajo sobre protección de datos del artículo 29. 160

5. Comisión Europea (2016) "Directrices sobre los delegados de protección de datos (DPO)". Adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017. Grupo de trabajo sobre protección de datos del artículo 29. Disponible en https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf (28/02/2021). 227, 415

6. Comisión Europea (2017). "La construcción de una economía de los datos europea". Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Disponible en https://eur-lex.europa.eu/content /news/ building_ EU_data_economy.html?locale=es (28/02/2021). 28

7.	Comisión Europea. "¿Qué es un responsable o encargado del tratamiento?" Web oficial de la Unión Europea. Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/ controller-processor/what-data-controller-or-data-processor_es. (28/02/2021).	199
8.	Comisión Europea. Web oficial de la Unión Europea. "¿Qué es una violación de la seguridad de los datos y qué deberíamos hacer en caso de sufrir una?". Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/ reform/rules-business-and-organisations/obligations/ what-data-breach-and-what-do-we-have-do-case-data-breach_es (31/01/2021).	209, 210 (2)
9.	Comisión Europea. Web oficial de la Unión europea. "Coronavirus: la Comisión propone un certificado digital verde " Disponible en https://ec.europa.eu/ commission/presscorner /detail/es/ip_21_1181 (15/04/2021).	439 (2)
10.	Comisión Europea. Web oficial de la Unión Europea. "Comité Europea de Protección de Datos". Disponible en https://edpb.europa.eu/about-edpb/about-edpb_es (28/02/2021).	182
11.	EPIETEN. "Programa Europeo de Formación en Epidemiología de Intervención". Disponible es https://www.eurosurveillance.org/ content/10.2807/ esm. 01.04.00171-es (28/02/2021).	164
12.	EUR Lex. "Jerarquía de normas de la Unión Europea (UE)" Web oficial de la Unión Europea Disponible en https://eur-lex.europa.eu/summary/glossary/ %20norms_ hierarchy. html? locale=es (31/01/2021).	84
13.	EUR Lex. Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre un marco para la emisión, verificación y aceptación de certificados de interoperabilidad de vacunación, pruebas y recuperación a los nacionales de terceros países que residan legalmente o residan legalmente en los territorios de los Estados miembros durante el COVID -19 pandemia (Certificado Verde Digital) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021PC0140&qid =1617357403450&from=EN. (30/04/2021).	439
14.	UE (7 diciembre 2000) "Carta de los Derechos Fundamentales de la Unión Europea" de (2010/C 83/02). C 83/402. Disponible en https://www.boe.es/ doue/ 2010/ 083/ Z00389-00403.pdf.	74
15.	YOUR EUROPE. "Reglamento general de protección de datos. ¿Cuándo se aplica el Reglamento general de protección de datos (RGPD)?". Web oficial de la UE. Disponible en https://europa.eu/youreurope/ business/dealing-with-customers/data-protection /data-protection-gdpr/index_es.htm (28/02/2021).	32
	Documentos de organizaciones internacionales (por orden alfabético)	Página/s
1.	CSDH (2008) "Closing the gap in a generation: health equity through action on the social determinants of health: Commission on Social Determinants of Health final report". WHO Commission on Social Determinants of Health. World Health Organization. Geneva, Switzerland: World Health Organization, Commission on Social Determinants of Health.	256
2.	ECDC. Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC). Comisión Europea. Web oficial de la Unión Europea. Disponible en https://europa.eu/ -union/ about-eu/agencies/ecdc_es (31/01/2021).	164 (2), 182

3.	Johns Hopkins University (11 marzo 2020) (28 octubre 2020) "COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE)" at Johns Hopkins University. Disponible en https://www.arcgis.com/apps/opsdashboard/index.html#/ bda7594740 fd40299423467b48e9ecf6 (28/10/2020).	163, 385
4.	MEDICOS SIN FRONTERAS. "Epidemias". Disponible en https://www.msf.es/nuestra-accion/epidemias (28/02/2021).	161
5.	OECD. Tracking and tracing COVID: protecting privacy and data while using APPS and Biometrics. OECD 2020. Updated 23 April 2020. Disponible en https://www.oecd.org/ coronavirus/policy-responses/ tracking-and-tracing-covid-protecting-privacy-and- data-while-using-apps-and-biometrics-8f394636/ (31/01/2021).	388
6.	OMS (20-30 mayo 1994) "Declaración para la promoción de los derechos humanos en Europa". Oficina regional para Europa. Disponible es https://www.ffis.es/ ups/ documentacion_ley_3_2009/ Declaracion_promocion_derechos_pacientes _en _ Europa.pdf (28/02/2021).	298
7.	OMS. Organización Mundial de la Salud "Quiénes somos". Disponible en https://www.who.int/es/about/who-we-are (28/02/2021).	254
8.	OMS (2005) "Reglamento Sanitario Internacional (2005)". Tercera edición. Disponible en https://www.who.int/ihr/publications/9789241580496/es/ (28/02/2021).	166
9.	OMS. Organización Mundial de la Salud (24 febrero 2010) "¿Qué es una pandemia?". Disponible https://www.who.int/csr/disease/swineflu/ frequently_ asked_ questions /pandemic/es/ (28/02/2021).	162
10.	OMS (2013). La 13ª Conferencia Internacional sobre la Evaluación de Impacto en la Salud. World Health Organitation. Health Promotion Switzerland. Université de Genève. Ginebra, 2-4 de octubre de 2013.	256
11.	OMS. (8 April 2020) "Advice on the use of point-of-care immunodiagnostic tests for COVID-19". World Health Organization. Scientific brief. Disponible en https://www.who.int/ docs/ default-source/ coronaviruse/ sb-2020-1-poc-immunodiagnostics-2020-04-08-e.pdf? sfvrsn=4c26ac39_2 (31/01/2021).	392
12.	OMS (2021) "Vacunas e inmunización: ¿qué es la vacunación?". Organización mundial de la saldu. Disponible en https://www.who.int/es/news-room/q-a-detail/vaccines-and-immunization- what-is-vaccination?adgroupsurvey={adgroupsurvey}&gclid= Cj0KCQjwi7yCBhDJARIsAMWFScP 4WVF8N3UJoZxMLdSWgCqNXy60u1U DPNgOv6YWN QOd6X0lma NTS WAaArglEALw_wcB. (28/02/2021).	259
13.	ONU (2016), "Derechos Humanos", Manual para Parlamentarios nº26. Oficina del Alto Comisionado. Naciones Unidad. Disponible en https://www.ohchr.org/Documents/ Publications/HandbookParliamentarians_SP.pdf (31/01/2021).	68
14.	OPS. (11 marzo 2020) "La OMS caracteriza a COVID-19 como una pandemia". Organización Panamericana de la Salud. OMS. Disponible en https://www.paho.org/ hq/index.php?option= com_content&view= article&id= 15756: who-characterizes-covid-19-as-a-pandemic&Itemid=1926&lang=es (28/02/2021).	163

Prensa (por orden alfabético) Página/s

1. BBC. Mundo.com "Coronavirus: las pandemias que pusieron al mundo en alerta en la historia reciente (y cómo se afrontaron)". Disponible en https://www.bbc.com/mundo/noticias-51843449 (28/10/2020). 163

2. BBC.Mundo.com (18 de diciembre de 2002), "Las razas no existen" Disponible en http://news.bbc.co.uk/hi/spanish/science/newsid_2585000/2585667.stm (28/02/2021). 52

3. BBC News (25 abril 2020) "Tests de coronavirus: cómo son las pruebas serológicas y moleculares para detectar el covid-19 y qué ventajas e inconvenientes". Disponible en https://www.bbc.com/mundo/noticias-52361548 (31/05/2020). 392

4. El Mundo (30 junio 2018) "Facebook reconoce la filtración de datos de más de 120 millones de usuario ".Disponible en https://www.elmundo.es/tecnologia/ 2018/06/30/ 5b35f2f4468aeb22438b457 d.html (31/05/2020). 252

5. El Mundo (26 agosto 2010) "Multa de 300.000 euros por tirar a la basura historias clínicas de 158 pacientes ginecológicas". Disponible en https://www.elmundo.es/ elmundo/ 2010/08/26/ andalucia_sevilla/1282812502.html (31/01/2021). 271

6. Infosalus (1 abril 2020) "Illa descarta que se vaya a crear un carnet de inmunidad del Covid-19 como ha hecho Castilla y León". Disponible en https://www.infosalus.com/ salud-investigacion/ noticia-illa-descarta-vaya-crear-carnet-inmunidad-covid-19-hecho-castilla-leon-20200408203016.html (31/01/2021). 394

7. La Vanguardia (25 abril 2020) "OMS: El "pasaporte de inmunidad" contra el COVID no tiene respaldo científico". Disponible en https://www.lavanguardia.com/vida /20200425/48714129316/oms-pasaporte-inmunidad-covid.html (31/01/2021). 395

Otras fuentes (por orden alfabético)

1. AEMM (8 mayo 2020). Asociación de Empresas del Metal de Madrid. Comunicado "Consideraciones sobre los controles de temperatura corporal y protección de datos en el marco de la crisis del COVID-19". Disponible en https://www.aecim.org/ consideraciones- sobre-los-controles-de-temperatura-corporal-y-proteccion-de-datos-en-el-marco-de-la-crisis-del-covid-19/# (31/05/2020). 389

2. AEC. (mayo 2020) "Mantenimiento". Disponible en https://www.aec.es/web/guest/ centro-conocimiento/mantenimiento (31/01/2021). 133

3. AEPap. (12 abril 2020). Asociación Española de Pediatría de Atención primaria "Pruebas diagnósticas de laboratorios de COIVD-19". Disponible en https://www.aepap.org/sites/default/files/documento/archivos-adjuntos/pruebas_diagnosticas_de_laboratorio_de_covid_vfinal.pdf (31/05/2020). 391, 392

4. CCOO (8 de mayo 2020) "CCOO exige la realización del test de Covid 19 de máxima fiabilidad al personal que trabaja en el sector de la dependencia". Comisiones Obreras de Andalucía 8 mayo 2020. Disponible en https://andalucia.ccoo.es/noticia:493424--CCOO_exige_la_realizacion_del_test_de_Covid_19_de_maxima_fiabilidad_al_personal_que_trabaja_en_el_ sector_de_la_dependencia&opc_id= 434bdbdecfdacb8f5f4e92b187bd73a0 (31/01/2021). 393

5. Consejo General de la Abogacía Española (6 marzo 2019) "Código Deontológico adoptado por el Estatuto General de la Abogacía Española". Disponible en 155

https://www.abogacia.es/wp-content/uploads/2019/05/Codigo-Deontologico-2019.pdf (31/05/2020).

6. Escuela Europea de Excelencia (31 mayo 2018) "Cómo realizar el tratamiento de riesgos según ISO 31000:2018". Disponible en https://www. Escuelaeuropea excelencia .com/ 2018/05/ como-realizar-el-tratamiento-de-riesgos-segun-iso-310002018/ (31/05/2020). 217

7. Fundación IO (21 marzo 2020) "Inmunología Clínica del COVID-19 Qué sabemos hasta ahora?". Disponible en https://fundacionio.com/2020/03/21/inmunologia-clinica-del-covid19-que-sabemos-hasta-ahora-por-el-dr-fernando-farinas/ (31/01/2021). 395

8. IDIS. Fundación Instituto para el Desarrollo e Integración de la Sanidad (2020) "Sanidad privada, aportando valor. Análisis de situación 2019". Madrid. La Fundación Instituto para el Desarrollo e Integración de la Sanidad (IDIS). Disponible en https://www.fundacionidis.com/informes/analisis-de-situacion-de-la-sanidad-privada/sanidad-privada-aportando-valor-analisis-de-situacion-2019 (31/01/2021). 293

9. IEEE Computer Society. (2005) "Computing Curricula 2005: The Overview Report" The Joint Task Force for Computing Curricula 2005. USA. ACM and IEEE 34

10. LegalToday por y para abogados (17 junio 2014) "Caso Google vs. España: los ciudadanos ante el "derecho al olvido". Disponible en http://www.legaltoday.com/ practica-juridica/civil/nuevas tecnologias/ caso-google-vs-espana-los-ciudadanos-ante-el-derecho-al-olvido (28/02/2021). 251

11. Periodistas en español.com (27 noviembre 1993) "Código Deontológico de la Federación de Asociaciones de Periodistas de España (FAPE)". Disponible en https://periodistas-es.com/politica-editorial/codigo-deontologico-de-la-fapev (31/05/2020). 151

12. Portal Clinic (12 marzo 2020) "Diagnóstico del Coronavirus SARS-CoV-2". Hospital Clinic de Barcelona. Disponible en https://www.clinicbarcelona.org/asistencia/enfermedades/covid-19/diagnostico (31/01/2021). 391

13. SEMI. "Salud y enfermedad ¿qué son?" Sociedad española de medicina Interna. Disponible en https://www.fesemi.org/informacion-pacientes/hemeroteca-salud/enfermedades/salud-y-enfermedad-que-son. (28/02/2021). 255

14. SEI (2 de abril de 2020) "Utilidad de la determinación de anticuerpos anti SARS-CoV-2. Propuesta de implementación como prueba diagnóstica, pronóstica y de desarrollo de inmunidad protectora". Sociedad Española de Inmunología. Versión 01. Disponible en https://www.micof.es/bd/archivos/archivo15001.pdf (31/01/2021). 392

15. Statistas. Global No.1 Business Data Platform (28 agosto 2019) "Distribución del número total de farmacias de España en 2018, por comunidad autónoma". Disponible en https://es.statista.com/estadisticas/629225/numero-de-farmacias-por-comunidades-autonomas-en-espana/ (31/05/2020). 446

16. UNIR. "Descubre en qué consiste el principio de jerarquía normativa en el ámbito jurídico, sus características y de qué forma se configura en España". Revista UNIR. Disponible en https://www.unir.net/derecho/revista/jerarquia-normativa/ (28/02/2021). 83

ANEXOS

Anexo [A] Cuadro comparativo de las expresiones semánticas que utiliza en relación a los datos el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales		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	
7	acceso a los datos	3	acceso a datos personales
1	acceso a los datos y documentos de la historia clínica		
			acceso a los datos personales de forma rápida
			acceso de las autoridades públicas a los datos personales
1	afectado especifique los datos		
126	Agencia Española de Protección de Datos.		
			auditorías de protección de datos
27	autoridad de protección de datos		
	autoridad de protección de datos de la Comunidad Autónoma		
2	respectiva		
29	autoridades autonómicas de protección de datos		
1	autoridades autonómicas de protección de datos personales		
8	autoridades de protección de datos		
6	bloqueo de los datos		
1	cantidad de datos	2	calidad de los datos
1	categoría especial de los datos		categorías de datos
1	categorías de datos objeto de tratamiento		
2	categorías especiales de datos	6	categorías especiales de datos personales
			categorías de destinatarios de los datos personales
			categorías de los datos de carácter personal
		3	certificación de la protección de datos
			cifrado de datos personales
1	circulación de estos datos		circulación de datos
			circulación de datos personales en la Unión
1	cláusulas tipo de protección de datos	3	cláusulas tipo de protección de datos
14	Comité Europeo de Protección de Datos	3	Comité Europeo de Protección de Datos
6	comunicación de datos		comunicación de datos personales
			conjuntos de datos personales
2	confidencialidad de los datos		
2	conservación de datos		conservación de los datos personales
	conservación de los datos bloqueados		
	conservar los datos identificativos		
	control sobre sus datos		
	control sobre sus datos personales		
	corresponsables del tratamiento de los datos		
	Cualificación del delegado de protección de datos		
	cuando la información contenga datos personales		
	Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados		
21	datos	9	datos
			datos dactiloscópicos
	datos anonimizados o seudonimizados		
	datos bloqueados		
	datos censales		
	datos con fines de archivo en interés público		
	datos concretos		
	datos de contacto		datos de contacto
		6	datos de contacto del delegado de protección de datos
		3	datos de contacto del responsable
			datos de localización
	datos de identificación		
	datos de identificación personal del paciente		
	datos de los afectados		
	datos de quien formule		
2	datos de tráfico		
	datos genéticos		datos genéticos
	datos genéticos o biométricos	3	datos biométricos
	datos hayan sido facilitados		
	datos identificativos con los clinicoasistenciales		
	datos identificativos de los pacientes		
	datos imprescindibles para identificar		
	datos inexactos		datos personales inexactos
			datos leal y transparente
3	datos necesarios		
	datos o documentos obtenidos		
	datos obtenidos		
2	datos de carácter personal		
19	datos personales	84	datos personales
	datos personales a gran escala		

	datos personales deben ser destruidos		
	datos personales rectificados		
			datos personales con fines de archivo en interés público
			datos personales con fines de investigación científica o histórica o estadísticos
			datos personales de documentos oficiales
			datos personales no sean accesibles
			datos personales que sean incompletos
		4	datos personales relativos a la salud
			datos relativos a la vida sexual
	datos referidos a un deudor		
	datos relacionados		
	datos relativos a la comisión de infracciones penales o administrativas		
	datos se refieran a deudas ciertas		
	datos serán exactos		
	datos serán suprimidos		
2	datos seudonimizados		
	datos seudonimizados o anonimizados		
	datos tributarios		
	datos únicamente se mantengan		
30	delegados de protección de datos	23	delegado de protección de datos
	derecho a la limitación del tratamiento		
2	derecho a la protección de datos personales	3	derecho a la protección de datos
2	derecho fundamental a la protección de datos		
2	destrucción de los datos		
			evaluación de impacto relativa a la protección de datos
			exactitud de los datos personales
			flujos de datos
	encargado de tratamiento a los datos personales		
	encargado del tratamiento podrá conservar, debidamente bloqueados, los datos		
2	exactitud de los datos		exactitud de los datos personales
	excluyendo del tratamiento los datos de los afectados		
			evaluación de impacto relativa a la protección de datos
	fuentes de las que procedieran los datos		
			flujos de datos
	gran cantidad de datos personales		
	inclusión de tales datos		
	inexactitud de los datos personales		
	información previa a la autoridad de protección de datos competente.		
	informaciones y datos		
	Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.		
	introducción de los datos		
	legislación de protección de datos		
5	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal		
7	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales		
2	libre circulación de estos datos	4	libre circulación de datos personales
	limitación del tratamiento de los datos impugnando		
	mantenimiento de los datos		
		3	marcas de protección de datos
9	materia de protección de datos personales	8	materia de protección de datos
		4	minimización de datos
	naturaleza de los datos		naturaleza de los datos personales
	no manipulación de los datos		
	normativa de protección de datos		
	normativa de protección de datos personales		
		2	obligaciones de protección de datos
	parte de los datos, derecho de acceso		
	permaneciendo bloqueados los datos		
2	plataformas de intermediación de datos		
	podrán recogerse previo consentimiento expreso de los afectados los datos		
			políticas de protección de datos
2	portabilidad de los datos	4	portabilidad de los datos
	posición del delegado de protección de datos		
2	principios de protección de datos		principios de protección de datos
			protección de datos a escala mundial
			protección de datos de conformidad
			protección de datos de las iglesias y asociaciones religiosas
	prohibición del tratamiento de datos		
16	protección de datos	20	protección de los datos
		20	protección de los datos personales
	protección de datos de los menores en Internet		
8	protección de datos personales		
	publicación o difusión de sus datos personales		
	puesta a disposición de los datos a los jueces y tribunales		

			recibir los datos personales
			recogida de datos personales
	rectificación o supresión de datos personales		
	registro completo de los datos		registros de datos personales
	registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar		
	reglamento general de protección de datos		
	reidentificación de los datos		
	responsable de datos		
	responsables y encargados del tratamiento de datos		
	reutilización de datos personales		
4	seguridad de los datos personales	13	seguridad de los datos personales
			Sello Europeo de Protección de Datos
			sellos de protección de datos
		4	sellos y marcas de protección de datos
			seudonimización de datos personales
	sin restricciones de datos personales		
	sistema de información crediticia con datos relativos		
		6	Supervisor Europeo de Protección de Datos
			tipo de datos personales
	tipos de datos		tipos de datos
	tráfico masivo de datos personales		
6	transferencia internacional de datos	5	transferencia de datos personales a terceros países
	transferencias de datos tributarios		
5	transferencias internacionales de datos		
		5	transferencia de datos personales
			transferencia de los datos personales dentro de un grupo empresarial
		2	tratamiento automatizado de datos personales
		11	transferencias de datos personales
50	tratamiento de datos	33	tratamiento de datos personales
	tratamiento de datos con fines de archivo		
	tratamiento de datos de contacto		
2	tratamiento de datos de la investigación en salud		
		2	tratamiento de datos genéticos
	tratamiento de datos de naturaleza penal		
	tratamiento de datos en el ámbito de la función estadística pública		
	tratamiento de datos relativos a infracciones y sanciones administrativas		
	tratamiento de los datos personales procedentes de las imágenes y sonidos		
	tratamiento de los datos referidos a sus deudores		
		2	tratamiento automatizado de datos personales
	tratamiento no automatizado de datos personales		tratamiento no automatizado de datos personales
	tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras		
	tratamiento se limite a los datos estrictamente necesarios		
	tratamiento total o parcialmente automatizado de datos personales		tratamiento total o parcialmente automatizado de datos personales
	tratamientos de datos de personas fallecidas		
2	tratamientos de datos de salud		
	tratamiento de datos personales en la investigación en salud		
	traten datos de menores de edad		
			tratamiento de datos leal y transparente
			tratamiento de datos personales de los trabajadores
			tratamiento de datos leal y transparente
			transmitir datos personales
3	uso de datos personales seudonimizados		
	uso de sus datos		
	utilización de los datos		
		2	violación de la seguridad de los datos personales
	utilizase los datos para sus propias finalidades		

Anexo [B] Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos. AEPD de 30 de abril de 2020

30 DE ABRIL DE 2020

Comunicado de la AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos

La AEPD expresa su preocupación por este tipo de actuaciones, que suponen una injerencia particularmente intensa en los derechos de los afectados y que se están realizando sin el criterio previo de las autoridades sanitarias.

La paulatina retirada de las medidas de confinamiento y limitación de la actividad económica y social está determinando la implantación de medidas encaminadas a prevenir nuevos contagios de COVID – 19.

Entre estas medidas se está incluyendo, aparentemente de forma generalizada y en muy variados entornos, la toma de temperatura de las personas para determinar la posibilidad de que puedan acceder a centros de trabajo, comercios, centros educativos u otro tipo de establecimientos o equipamientos.

En esta situación, la Agencia Española de Protección de Datos considera necesario destacar su preocupación por este tipo de actuaciones, que se están realizando sin el criterio previo y necesario de

las autoridades sanitarias.

Tratamiento de datos personales sensibles

Debe señalarse, en primer lugar, que este tipo de operación supone un tratamiento de datos personales que, como tal, debe ajustarse a las previsiones de la legislación correspondiente. Esta normativa contiene apartados específicos que contemplan situaciones como la actual, al tiempo que permiten seguir aplicando los principios y garantías que protegen el derecho fundamental a la protección de datos.

Este tratamiento de toma de temperatura supone una injerencia particularmente intensa en los derechos de los afectados. Por una parte, **porque afecta a datos relativos a la salud de las personas**, no sólo porque el valor de la temperatura corporal es un dato de salud en sí mismo sino también porque, a partir de él, se asume que una persona padece o no una concreta enfermedad, como es en estos casos la infección por coronavirus.

Por otro lado, los controles de temperatura se van a llevar a cabo **con frecuencia en espacios públicos**, de forma que una eventual denegación de acceso a un centro educativo, laboral o comercial estaría desvelando a terceros que no tienen ninguna justificación para conocerlo que la persona afectada tiene una temperatura por encima de lo que se considere no relevante y, sobre todo, que puede haber sido contagiada por el virus.

En último extremo, y dependiendo del contexto en que se aplique esta medida, las consecuencias de una posible denegación de acceso pueden tener un importante impacto para la persona afectada.

Criterios de implantación

La aplicación de estas medidas y el correspondiente tratamiento de datos requeriría la **determinación previa que haga la autoridad sanitaria competente**, que en estos momentos es el Ministerio de Sanidad, de su necesidad y adecuación al objetivo de contribuir eficazmente a prevenir la diseminación de la enfermedad en los ámbitos en los que se apliquen, regulando los límites y garantías específicos para el tratamiento de los datos personales de los afectados.

En ese sentido, debe tenerse en cuenta, entre otras cuestiones, que según las informaciones proporcionadas por las autoridades sanitarias, hay un porcentaje de personas contagiadas asintomáticas que no presenta fiebre, que la fiebre no siempre es uno de los síntomas presentes en pacientes sintomáticos, en particular en los primeros estadios del desarrollo de la enfermedad, y que, por otro lado, puede haber personas que presenten elevadas temperaturas por causas ajenas al coronavirus.

Es por ello que estas medidas deben aplicarse solo atendiendo a los criterios definidos por las autoridades sanitarias, tanto en lo relativo a su utilidad como a su proporcionalidad, es decir, hasta qué punto esa utilidad es suficiente para justificar el sacrificio de los derechos individuales que las medidas suponen y **hasta qué punto estas medidas podrían o no ser sustituidas, con igual eficacia, por otras menos intrusivas.**

Por otro lado, esos criterios deben incluir también precisiones sobre los aspectos centrales de la aplicación de estas medidas. Así, por ejemplo, la temperatura a partir de la cual se consideraría que una persona puede estar contagiada por la COVID – 19 debería establecerse atendiendo a la evidencia científica disponible. No debería ser una decisión que asuma cada entidad que implante estas prácticas, ya que ello supondría una aplicación heterogénea que disminuiría en cualquier caso su eficacia y podría dar lugar a discriminaciones injustificadas.

Principio de legalidad

Como todo tratamiento de datos, la recogida de datos de temperatura debe regirse por los principios establecidos en el Reglamento General de Protección de Datos (RGPD) y, entre ellos, el principio de legalidad. Este tratamiento debe basarse en una causa legitimadora de las previstas en la legislación de protección de datos para las categorías especiales de datos (artículos 6.1 y 9.2 del RGPD).

En el caso de la comprobación de la temperatura corporal como medida preventiva de la expansión de la COVID – 19, **esa base jurídica no podrá ser, con carácter general, el consentimiento de los interesados**. Las personas afectadas no pueden negarse a someterse a la toma de temperatura sin perder, al mismo tiempo, la posibilidad de entrar en unos centros de trabajo, educativos o comerciales, o en los medios de transporte, a los que están interesados en acceder. Por tanto, ese consentimiento no sería libre, uno de los requisitos necesarios para invocar esta base legitimadora.

En el **entorno laboral**, y siempre que se hayan tenido en consideración las demás cuestiones que se abordan en esta comunicación, la posible base jurídica podría encontrarse en la obligación que tienen los empleadores de garantizar la seguridad y salud de las personas trabajadoras a su servicio en los aspectos relacionados con el trabajo. Esa obligación operaría a la vez como excepción que permite el tratamiento de datos de salud y como base jurídica que legitima el tratamiento.

Sin embargo, y adicionalmente, el RGPD requiere también en estos casos que la norma que permita este tratamiento ha de establecer también **garantías adecuadas**. Dichas garantías habrán de ser especificadas por el responsable del tratamiento.

Esa base jurídica podría ser tenida en cuenta con un alcance amplio, atendiendo a que, aunque un centro o local estén destinados a unas finalidades específicas que impliquen que en ellos se concentren un elevado número de clientes o usuarios ajenos a la empresa que los gestiona, siempre estarán presentes en ellos personas trabajadoras sobre las que el empleador mantiene sus obligaciones.

Esta aproximación, no obstante, requiere de una adecuada ponderación entre el impacto sobre los derechos de los clientes o usuarios de estas medidas y el impacto en el nivel de protección de las personas empleadas. Esa ponderación debe basarse en diferentes factores. Ante todo, los criterios establecidos por las autoridades sanitarias. Pero también los relacionados con el mayor o menor riesgo que se pueda producir en cada caso concreto o con la posibilidad de aplicar medidas alternativas de protección para el personal. Por ejemplo, el riesgo será menor en un establecimiento en el que las personas empleadas estén físicamente separadas de la clientela que en otro en que esa barrera física no exista o sea más precaria.

En otros ámbitos en que no sea relevante esta base jurídica, cabría plantear la existencia de intereses generales en el terreno de la salud pública que deben ser protegidos. No obstante, esta posibilidad requeriría igualmente, como establece el artículo 9.2.i RGPD, de **un soporte normativo a través de leyes** que establezcan ese interés y que aporten las garantías adecuadas y específicas para proteger los derechos y libertades de los interesados.

La utilización del **interés legítimo** de los responsables del tratamiento como base legitimadora quedaría en todo caso excluida, por un doble motivo. Por una parte, porque ninguna disposición del artículo 9.2 del RGPD permite levantar la prohibición de tratamiento de datos sensibles por razones de interés legítimo (salvo que en determinadas materias así lo contemple el derecho de la Unión o de los Estados Miembro). Por otra, porque el impacto de este tipo de tratamientos sobre los derechos, libertades e intereses de los afectados haría que ese interés legítimo no resultara prevalente con carácter general.

Limitación de finalidad y exactitud de los datos

La normativa de protección de datos contiene otras disposiciones que resultan también especialmente aplicables en el caso de las mediciones de temperatura como medida de prevención contra la expansión de la COVID – 19.

Entre los principios de protección de datos recogidos en el RGPD, debe mencionarse el de limitación de la finalidad. Este principio supone que los datos (de temperatura) solo pueden obtenerse con la finalidad específica de detectar posibles personas contagiadas y evitar su acceso a un determinado lugar y su contacto dentro de él con otras personas. Pero esos datos no deben ser utilizados para ninguna otra finalidad. Esto es especialmente aplicable en los casos en que la toma de temperatura se realice utilizando dispositivos (como, por ejemplo, cámaras térmicas) que ofrezcan la posibilidad de grabar y conservar los datos o tratar información adicional, en particular, información biométrica.

De igual modo, el principio de exactitud, aplicado en este contexto, implica que los equipos de medición que se empleen deben ser los adecuados para poder **registrar con fiabilidad** los intervalos de temperatura que se consideren relevantes. Esta adecuación debiera establecerse utilizando solo equipos homologados para estos fines y con criterios que tengan en cuenta esos niveles de sensibilidad y precisión. El personal que los emplee debe reunir los requisitos legalmente establecidos y estar formado en su uso. Conviene insistir, a este respecto, en el impacto que sobre los interesados tendría que la identificación de un posible indicador de la existencia de contagio resultara errónea como consecuencia de un equipo inapropiado o de un mal desarrollo de la medición.

Derechos y garantías

En todo caso, los afectados siguen manteniendo sus derechos de acuerdo con el RGPD y siguen siendo de aplicación las demás garantías que el Reglamento establece, si bien adaptadas a las condiciones y circunstancias específicas de este tipo de tratamiento.

En ese sentido, debieran considerarse, entre otras, **medidas relativas a la información** a los trabajadores, clientes o usuarios sobre estos tratamientos (en particular si se va a producir una grabación y conservación de la información), u otras para permitir que las personas en que se detecte una temperatura superior a la normal puedan reaccionar ante la decisión de impedirles el acceso a un

recinto determinado (por ejemplo, justificando que su temperatura elevada obedece a otras razones). Para ello, el personal deberá estar cualificado para poder valorar esas razones adicionales o debe establecerse un procedimiento para que la reclamación pueda dirigirse a una persona que pueda atenderla y, en su caso, permitir el acceso.

Es igualmente importante establecer los **plazos y criterios de conservación** de los datos en los casos en que sean registrados. En principio, y dadas las finalidades del tratamiento, este registro y conservación no debieran producirse, salvo que pueda justificarse suficientemente ante la necesidad de hacer frente a eventuales acciones legales derivadas de la decisión de denegación de accesos.

Debe señalarse, por último, que esta comunicación se refiere con carácter general a cualquier proceso de toma de temperatura en los escenarios más probables en este periodo de mitigación del confinamiento y limitaciones a la movilidad y a la actividad social y económica.

Sin embargo, dependiendo del tipo de tecnología que se emplee, puede ser necesario tomar en consideración otros elementos que, aunque relacionados con los mencionados, tienen una especial incidencia en una u otra de esas diferentes tecnologías.

Este es el caso de las **cámaras térmicas**, a las que ya se ha hecho alusión, en la medida en que pueden ofrecer posibilidades adicionales a la toma de temperatura y que, por ello, deben ser utilizadas prestando especial atención a los principios de limitación de finalidad y minimización de datos establecidos por el artículo 5.1 RGPD.

Anexo [C] Listado de tipos y subtipos de datos, en base a su utilización

Tipos de datos	
Datos	**Concepto y ubicación**
anonimizados	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no lo utiliza.
	La Ley Orgánica 2/2018 en el punto 2 de la Disposición adicional decimoséptima al referirse a los Tratamientos de datos de salud, lo hace junto al término "seudonimizados". Utiliza la expresión cuando puedan excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.
biométricos[C]	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	La Ley Orgánica 2/2018 utiliza dato biométrico en la Disposición final undécima (Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno) para diferenciarlo del dato genético. El Reglamento 2016/679 (UE) define como dato biométrico: *datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*.
	El Reglamento 2016/679 (UE) hace referencia al "dato biométrico" en el artículo 9 (Tratamiento de categorías especiales de datos personales), en todo caso las diferencias de los datos de salud y los datos genéticos.
bloqueados	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no lo utiliza.
	Estos datos son utilizados por la Ley Orgánica 2/2018 en primer lugar en el artículo 30 (Bloqueo de datos): *El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.*
	El artículo 33 (El encargado del tratamiento) se refiere que los datos deberán ser conservados por el encargado del tratamiento cuando entre este y el responsable pudieran derivarse responsabilidades.

	El artículo 20 (Sistemas de información crediticia) dice que las entidades crediticias mantendrán bloqueados los datos mientras transcurra el periodo de notificación al interesado, por incumplimiento de sus obligaciones crediticias.
carácter personal, de	Estos datos son utilizados por el Reglamento 2016/679 (UE). La Ley Orgánica 2/2018 no los utiliza.
	La Ley Orgánica 2/2018 solo utiliza "dato de carácter personal" al referirse a la denominación de la Ley Orgánica 15/1999, de 13 de diciembre (ya derogada).
	El Reglamento 2016/679 (UE) utiliza la expresión "datos de carácter personal" en los Considerando en veinticuatro (24) ocasiones. En su articulado la utiliza en una sola ocasión para referirse a la denominación del El Reglamento (CE) n.o 45/2001 y en el artículo 4 (definiciones) al definir la limitación del tratamiento, diciendo que es "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro".
censales	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 utiliza "dato censal" en la Disposición final tercera (Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General).
clínico-asistenciales	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	En la Ley Orgánica 2/2018 aparece este concepto, dato clínico-asistencial, inferidamente en el Disposición final novena (Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica) al diferenciarlos de los datos identificativos del paciente.
concretos	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 utiliza el término "dato concreto" en el artículo 20 (Sistemas de información crediticia) en el siguiente sentido: *cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado*.

contacto, de	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	La Ley Orgánica 2/2018E utiliza la expresión "datos de contacto" en su artículo 19 (Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales). La calificación de "dato de contacto" se aplica en aquellos datos que permiten la localización personal (y no profesional) del afectado en los supuestos del artículo 6 del Reglamento (UE) 2916/679.
	El Reglamento 2016/679 (UE) hace referencia a "datos de contacto" como aquellos que permitan identificar al responsable o al encargado del tratamiento o al delegado de protección de datos.
	El Reglamento 2016/679 (UE) hace referencia a los "datos de contacto" del responsable y del encargado del tratamiento en los artículos 13, 14 y 30, mientras que en relación al delegado de protección de datos aparece en los artículos 13,14, 33, 36 y 37.
exactos	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 hace uso de la expresión "datos exactos" en el artículo 4 (Exactitud de los datos), cuando se refiere en su TÍTULO II a los principios de protección de datos. Si bien es cierto que el artículo 4 de le Ley no se refiere al dato personal sino al dato, también es cierto que se remite al artículo 5 del Reglamento en donde si cita al dato personal.
	El Reglamento 2016/679 (UE) lo hace en su artículo 5 (Principios relativos al tratamiento) situando al "dato exacto" como un principio del tratamiento de los datos.
	Ambas normas los contraponen a los datos inexactos que son contrarios al derecho de la persona titular de los datos. El dato será exacto por imperativo legal, así lo dice el artículo 4 de la Ley Orgánica y el artículo 5 del Reglamento, al decir este último que los datos personales serán exactos, lo que significa que el dato inexacto es ilícito.
facilitados	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 utiliza el calificativo de "facilitado" en su artículo 4 (Exactitud de los datos), artículo 20 (Sistemas de información crediticia), artículo 87 (Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral) y artículo 94 (Derecho al olvido en servicios de redes sociales y servicios equivalentes). La norma hace uso de "dato facilitado" para hacer énfasis en que ha sido aportado bien, por el interesado o bien, por un tercero, pero que en todo caso ha sipo aportado por alguien, es decir, en consecuencia, no ha sido obtenido por otra vía. Pueden haber sido facilitados por el interesado o titular de los mismos o por una tercera persona, lo cual cambia el principio que

	regula el tratamiento. Al "dato facilitado" se le contrapone el dato obtenido, excepto cuando la norma indica explícitamente que han sido obtenidos del afectado (artículo 11. Transparencia e información al afectado).
fines de interés público, con	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	El Reglamento 2016/679 (UE) utiliza la expresión "datos personales con fines de archivo en interés público" al igual que lo hace la Ley Orgánica 2/2018.
	La Ley Orgánica 2/2018 lo utiliza en artículo 26 (Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas). Realmente, el calificativo de público se refiere al tratamiento de archivos con fines de interés público, no a que el dato tenga naturaleza pública.
	EL Reglamento 2016/679 (UE) lo utiliza en artículo 5 (Principios relativos al tratamiento) al referirse a que el tratamiento ulterior de los "datos personales con fines de archivo en interés público", fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»).
genéticos	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	La Ley Orgánica 2/2018 utiliza "dato genético" en la Disposición adicional decimoséptima (Tratamientos de datos de salud) y en la Disposición final undécima (Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno). Utiliza el calificativo de dato genético para diferenciarlo del dato de salud.
	El Reglamento 2016/679 (UE) lo utiliza en el artículo 9 (Tratamiento de categorías especiales de datos personales). El Reglamento 2016/679 (UE) define "dato genético" como: *los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.* Además, se el dato genético se diferencia del dato se salud y del dato biométrico.
identificación, de	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.

	La Ley Orgánica 2/2018 hace uso de la expresión "datos de identificación de los interesados" en la Disposición adicional decimoséptima (Tratamientos de datos de salud) punto 2 letra f) . En este artículo hace referencia a que en los trabajos de investigación en el sector de la salud puede haber datos que identifiquen a las personas sujetos de dicha investigación, y hay que tomar medidas para garantizar que los investigadores no tengan acceso a estos datos de identificación.
identificación personal del paciente, de	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 en la Disposición final novena (Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica) utiliza la expresión "datos de identificación personal del paciente" como aquellos que permiten identificarle en sus rasgos personales y que deberán estar separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. También utiliza la forma, datos identificativos de los pacientes.
	La Reglamento 2016/679 (UE) utiliza la expresión "datos personales de pacientes" solo en el Considerando 91, mientras que en el texto articulado no hace mención a tal expresión.
imágenes y sonidos, datos personales procedentes de las	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 utiliza la expresión "datos personales procedentes de las imágenes y sonidos" en el artículo 22 (Tratamientos con fines de videovigilancia). Esta expresión viene a corroborar las definiciones que sobre "el dato" se han venido plasmando en este documento, en la medida que imágenes y sonido también son datos y más concretamente un tipo de dato.
	El Reglamento 2016/679 (UE) no utiliza esta expresión, si bien define que en datos biométricos incluye a las imágenes faciales o datos dactiloscópicos[C].
imprescindibles para identificar	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no lo utiliza.
	La Ley Orgánica 2/2018 utiliza el calificativo de "datos imprescindibles" en su artículo 23 (Sistemas de exclusión publicitaria) como aquellos que deberán ser excluidos, al ser imprescindibles para identificar a los afectados.
incompletos	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.

	La Ley Orgánica 2/2018 hace referencia al "dato incompleto" en su artículo 14 (Derecho de rectificación) al mencionar que al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o *carácter incompleto de los datos* objeto de tratamiento. De tal forma que más que hablar de dato incompleto habla del carácter incompleto de un determinado dato.
	El Reglamento 2016/679 (UE) hace mención a " personales que sean incompletos" en su artículo 16 (Derecho de rectificación), de esta forma reconoce la existencia de datos incompletos, más que cierto carácter incompleto del dato.
inexactos	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	La Ley Orgánica 2/2018 hace uso de la expresión "datos inexactos" en su artículo 4 (Exactitud de los datos) y en sus artículos 93 (Derecho al olvido en búsquedas de Internet) y 94 (Derecho al olvido en servicios de redes sociales y servicios equivalentes) y lo hace de forma diferida al referirse a la información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo.
	El Reglamento 2016/679 (UE) usa el "dato inexacto" en el artículo 5 (Principios relativos al tratamiento) y artículo 16 (Derecho de rectificación) para apelar al carácter del dato que lo hace subsidiario bien del derecho de rectificación o bien del principio de exactitud del tratamiento de datos.
localización, de	Estos datos son utilizados por el Reglamento 2016/679 (UE). La Ley Orgánica 2/2018 no los utiliza.
	El Reglamento 2016/679 (UE) utiliza la expresión "datos de localización" en la el artículo 4 (definiciones) al definir los datos personales, que a su vez define a las personas identificables como toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
menores de edad, tratamiento de datos de	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 utiliza "datos de menores de edad" como un tipo distinto de dato, al cual hace referencia en los artículos 7 (Consentimiento de los menores de edad), 34 (Designación de un

	delegado de protección de datos) y 73 (Infracciones consideradas graves). En todo caso se refiere a datos de personas menores de edad.
	El Reglamento 2016/679 (UE) hace referencia al niño, pero tan solo en una ocasión utiliza la expresión “datos personales de niños” y lo hace en el Considerando 38. De forma inferida en el Considerando 78.
necesarios	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	La Ley Orgánica 2/2018 hace uso de la expresión "datos necesarios" en el artículo 19 (Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales) y artículo 53 (Alcance de la actividad de investigación) para identificar lo que entiende que son datos necesarios para determinados tratamientos.
	El Reglamento 2016/679 (UE) como "datos personales necesarios" aparecen en el Considerando 31, 68 y 162 y en el artículo 17 Derecho de supresión («el derecho al olvido») y artículo 25 (Protección de datos desde el diseño y por defecto)
obtenidos, datos o documentos	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	La Ley Orgánica 2/2018 hace referencia a los "datos obtenidos" en el artículo 11 (Transparencia e información al afectado) y artículo 22 (Tratamientos con fines de videovigilancia) y artículo 90 (Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral) cuando quiere resaltar la procedencia bien los datos obtenidos a través de sistemas o los datos obtenidos del propio afectado. También aparece en la Disposición final séptima (Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil). Frente a datos obtenidos utiliza datos facilitados.
	El Reglamento 2016/679 (UE) hace referencia a "datos obtenidos" en el artículo 4 (Definiciones) y artículo 14 (Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado) al querer identificar el origen del dato o si su procedencia es el propio interesado.
personales	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	La Ley Orgánica 2/2018 utiliza "datos personales" en 19 ocasiones, pero en ningún caso los define. Es curioso que en el artículo 1 (Objeto de la ley) la norma remita el "dato personal" al artículo 18.4 de la Constitución, el cual dice *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos,* al referirse al derecho fundamental de las personas físicas a la protección de datos personales. Lo cual parece que para el artículo 1 de la Ley Orgánica dato personal es el dato en informática.

	El Reglamento 2016/679 (UE) utiliza "datos personales" en 84 ocasiones, y los define en su artículo 4 como toda información sobre una persona física identificada o identificable («el interesado»), añadiendo que se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
rectificados, personales	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 hace referencia a un tipo de dato, el "dato personal rectificado", en el artículo 74 (Infracciones consideradas leves) cuando hace referencia a aquel que haya sido rectificado dentro de la obligación de informar al afectado.
salud, tratamiento de datos de (datos en el ámbito de la salud)	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza
	La Ley Orgánica 2/2018 utiliza la expresión "datos de salud" en la Disposición adicional decimoséptima (Tratamientos de datos de salud) y en la Disposición transitoria sexta (Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley) remitiendo el tratamiento de los "datos de salud" a la amplia legislación que sobre la materia existe en el ordenamiento jurídico español. La expresión "datos en el ámbito de la salud" se utiliza en el artículo 9 (Categorías especiales de datos). Aunque de forma implícita este artículo cataloga al dato de salud como de categoría especial, aunque explícitamente no lo hace.
	El Reglamento 2016/679 (UE) hace mención a "datos relativos a la salud" en el artículo 4 (Definiciones) y dice que son datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. El artículo 9 (Tratamiento de categorías especiales de datos personales) los cataloga como categoría especial de dato. El Considerando 35 dice, al respecto: *entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el*

	historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.
salud, tratamiento de datos en la investigación de la	Estos datos son utilizados por el Reglamento 2016/679 (UE). La Ley Orgánica 2/2018 no lo utiliza.
	En la Ley Orgánica 2/2018 aparece en el dato de salud aplicado a la investigación sanitario en la Disposición adicional decimoséptima (Tratamientos de datos de salud); Disposición transitoria sexta (Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica) y en Disposición final quinta (Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad)
	En el Reglamento 2016/679 (UE) aparece el concepto investigación científica, sin embargo, siempre de forma inferida y no directa, pues no aparee la expresión dato de investigación científica
seudonimizado	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza
	La Ley Orgánica 2/2018 utiliza el concepto de "datos personales seudonimizados" en la Disposición adicional decimoséptima (Tratamientos de datos de salud)
	El Reglamento 2016/679 (UE) utiliza "dato personal seudonimizado" en el Considerando 26. Utiliza con más frecuencia la expresión de "seudonimización a los datos personales", que de alguna forma crea el dato personal seudonimizado. Entiende por dato seudonimizado: *cuando se utiliza en un tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.*
tráfico, de	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.
	La Ley Orgánica 2/2018 hace uso de la expresión "los datos de tráfico" en su artículo 52 (Deber de colaboración) y en la Disposición adicional decimocuarta (Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE) y hace referencia al dato que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
tributarios	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) no los utiliza.

	La Ley Orgánica 2/2018 utiliza "dato tributario" en la Disposición adicional decimotercera (Transferencias internacionales de datos tributarios).
vida sexual, datos relativos a la	Estos datos son utilizados por la Ley Orgánica 2/2018. El Reglamento 2016/679 (UE) también los utiliza.
	La Ley Orgánica 2/2018 utiliza "datos personales que hagan referencia a la vida sexual" en la Disposición final undécima (Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno) y de forma inferida en el artículo 9 (Categorías especiales de datos). Son datos de categoría especial.
	El Reglamento 2016/679 (UE) usa la expresión "datos relativos a la vida sexual" en el artículo 9 (Tratamiento de categorías especiales de datos personales). Son datos de categoría especial.

Anexo [D] Tabla comparativa de los derechos que aparecen en el Reglamento (UE) 2016/679 y los que aparecen en la Ley Orgánica 3/2018

Reglamento (UE) 2016/7679	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
CAPÍTULO III. Derechos del interesado	Título III. Derechos de las personas
	Capítulo I. Transparencia e información
Sección 1. Transparencia y modalidades	
Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado	Artículo 11. Transparencia e información al afectado
1.El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios. 4.5.2016 L 119/39 Diario Oficial de la Unión Europea ES 2.El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.3.El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo. 4.Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales. 5.La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados	1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. 2. La información básica a la que se refiere el apartado anterior deberá contener, al menos: a) La identidad del responsable del tratamiento y de su representante, en su caso. b) La finalidad del tratamiento. c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679. Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679. 3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también: a) Las categorías de datos objeto de tratamiento. b) Las fuentes de las que procedieran los datos.

para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud. 6.Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado. 7.La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente. 8.La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la	
	Capítulo II. Ejercicio de los derechos
Sección 2. Información y acceso a los datos personales	
	Artículo 12. Disposiciones generales sobre ejercicio de los derechos
	1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario. 2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio. 3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule. 4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable. 5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas. 6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica. 7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado	
1.Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero; e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado. 2.Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; d) el derecho a presentar una reclamación ante una autoridad de control; e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos; f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. 3.Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.	

4.Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.		
Artículo 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado		
1.Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento; d) las categorías de datos personales de que se trate; e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado. 2.Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado: a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo; b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero; c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada; e) el derecho a presentar una reclamación ante una autoridad de control; f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público; g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. 3.El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2: a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos; b) si los datos personales han de utilizarse para comunicación con el		

interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez. 4.Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2. 5.Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que: a) el interesado ya disponga de la información; b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información; c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria. 4.5.2016 L 119/42 Diario Oficial de la Unión Europea ES	
Artículo 15. Derecho de acceso del interesado	**Artículo 13. Derecho de acceso**
1.El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información: a) los fines del tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; f) el derecho a presentar una reclamación ante una autoridad de control; g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa	1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679. Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud. 2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho. No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. 2.Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia. 3.El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. 4.El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.	3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello. 4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.
Sección 3. Rectificación y supresión	
Artículo 16. Derecho de rectificación	**Artículo 14. Derecho de rectificación**
El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.	Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.
Artículo 17. Derecho de supresión («el derecho al olvido»)	**Artículo 15. Derecho de supresión**
1.El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1. 2.Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén	1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679. 2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. 3.Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones.	
Artículo 18. Derecho a la limitación del tratamiento	**Artículo 16. Derecho a la limitación del tratamiento**
1.El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. 2.Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. 3.Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.	1.El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679. 2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.
Artículo 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento	
El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado	

los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.	
Artículo 20. Derecho a la portabilidad de los datos	**Artículo 17. Derecho a la portabilidad**
1.El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados. 2.Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3.El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. 4.El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.	El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679
Sección 4. Derecho de oposición y decisiones individuales automatizadas	
Artículo 21. Derecho de oposición	**Artículo 18. Derecho de oposición**
1.El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. 2.Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. 3.Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines. 4.A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.	El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas. 6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.		
Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles		
1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. 2. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado. 3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. 4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.		

Anexo E Formulario de rectificación

EJERCICIO DERECHO DE RECTIFICACIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de rectificación: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de rectificación, de conformidad con lo previsto en el artículo 16 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA

Que se proceda a acordar la rectificación de los datos personales, que se realice en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Datos sobre los que solicito el derecho de rectificación:

Que en caso de que se acuerde que no procede practicar la rectificación solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

Asimismo, en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta rectificación a los mismos.

En .....a.....de.....de 20.....

Firmado:

INSTRUCCIONES

1. Este modelo se utilizará para el caso de que se deban rectificar datos inexactos o incompletos por parte del responsable del tratamiento.

2. Para probar el carácter inexacto o incompleto de los datos que se estén tratando resulta necesaria la aportación de la documentación que lo acredite al responsable del tratamiento.

3. Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

4. La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

5. El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

6. Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho de rectificación, resulta necesario que hayan transcurrido un mes sin que el responsable haya respondido a su petición, y aporte alguno de los siguientes documentos:

• la negativa del responsable del tratamiento a la rectificación de los datos solicitados.

• copia sellada por el responsable del tratamiento del modelo de petición de rectificación.

• copia del modelo de solicitud de rectificación sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

• cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

Anexo F Formulario de limitación

EJERCICIO DEL DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de limitación: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico ……..,por medio del presente escrito ejerce el derecho de limitación, de conformidad con lo previsto en el artículo 18 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITO

Que se limite el tratamiento de mis datos personales, teniendo en consideración:

☐ Que el tratamiento es ilícito y me opongo a su supresión.

☐ Que el responsable ya no necesita mis datos personales para los fines para los cuales fueron recabados, pero los necesito para la formulación, ejercicio o defensa de mis reclamaciones.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes, y que se comunique esta limitación a cada uno de los destinatarios que ese responsable del tratamiento haya comunicado mis datos personales.

En .....a.....de.....de 20.....

Firmado:

INSTRUCCIONES

1. Este modelo se utilizará por el afectado que desee solicitar al responsable que limite el tratamiento de sus datos personales cuando proceda alguna de las siguientes situaciones:

- El tratamiento de sus datos personales es ilícito y el afectado se oponga a la supresión de sus datos personales;

-El responsable ya no necesita los datos personales para los fines del tratamiento, pero el afectado los necesita para la formulación, el ejercicio o defensa de sus reclamaciones.

2. Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

3. La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

4. El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

5. Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho a la limitación del tratamiento en el plazo máximo de un mes, y aporte alguno de los siguientes documentos:

•la negativa del responsable del tratamiento a la limitación del tratamiento de los datos solicitados.

•copia sellada por el responsable del tratamiento del modelo de petición de limitación del tratamiento.

•copia del modelo de solicitud de limitación del tratamiento sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

•cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

Anexo G Formulario de portabilidad

EJERCICIO DEL DERECHO A LA PORTABILIDAD DE LOS DATOS

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que ejercita el derecho a la portabilidad de los datos: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico ..... por medio del presente escrito ejerce el derecho la la portabilidad de los datos, de conformidad con lo previsto en el artículo 20 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITA

Que se le faciliten en el plazo de un mes sus datos personales en un formato estructurado, de uso común y lectura mecánica.

En su caso, que los citados datos personales sean transmitidos directamente al responsable .....(especifíquese nombre o razón social), siempre que sea técnicamente posible.

En .....a.....de.....de 20.....

Firmado

INSTRUCCIONES

1. El Modelo se utilizará por el afectado que desee que se le faciliten sus datos personales en un formato estructurado, de uso común y lectura mecánica.
También podrá emplearse si quisiera que los citados datos personales sean transmitidos directamente de responsable a responsable cuando sea técnicamente posible.

2. Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

3. La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

4. El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

5. Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho a la portabilidad de datos en el plazo de un mes, y aporte alguno de los siguientes documentos:

•la negativa del responsable del tratamiento a la portabilidad de los datos solicitados.

•copia sellada por el responsable del tratamiento del modelo de petición de portabilidad.

•copia del modelo de solicitud de portabilidad sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

•cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

Anexo H Formulario de oposición

EJERCICIO DEL DERECHO DE OPOSICIÓN (Modelo A)

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de oposición: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de oposición previsto en el artículo 21 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITO

La oposición al tratamiento de mis datos personales, teniendo en consideración que:

☐ El tratamiento de mis datos personales se basa en una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, debiendo limitarse el tratamiento de los mismos hasta que obtenga respuesta del ejercicio de este derecho.

☐ El tratamiento de mis datos personales se basa en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero, debiendo limitarse el tratamiento de los mismos hasta que se obtenga respuesta del ejercicio de este derecho.

☐ El tratamiento de mis datos personales se está realizando con fines de investigación científica o histórica o fines estadísticos.

Sin perjuicio de que corresponde al responsable del tratamiento acreditar motivos legítimos imperiosos que prevalezcan sobre mis intereses, derechos y libertades (en los dos primeros supuestos), o una misión realizada en interés público (en el tercer supuesto), acredito como situación personal para oponerme al tratamiento de mis datos personales

.....

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

En .....a.....de.....de 20.....

Firmado:

EJERCICIO DEL DERECHO DE OPOSICIÓN (Modelo B)

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de oposición: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de oposición previsto en el artículo 21 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITO

La oposición al tratamiento de mis datos personales con fines de mercadotecnia, incluyendo la elaboración de perfiles sobre mi persona.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

En .....a.....de.....de 20.....

Firmado:

INSTRUCCIONES

1. El modelo A se utilizará cuando el afectado desee oponerse al tratamiento de sus datos personales, por motivos relacionados con su situación particular, en cualquiera de las siguientes situaciones:

-El tratamiento de sus datos personales se está realizando en base a una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

-El tratamiento de mis datos personales se está realizando en base a la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero.

En estos dos primeros supuestos, el mero ejercicio del derecho de oposición conlleva la limitando

-El tratamiento de mis datos personales se está realizando con fines de investigación científica o histórica o fines estadísticos.

El modelo B. se utilizará cuando el afectado desee oponerse al tratamiento de sus datos personales con fines de mercadotécnica directa, incluyendo la elaboración de perfiles.

2. Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

3. La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

4. El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

5. Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho de oposición, resulta necesario que hayan transcurrido un mes sin que el responsable haya hecho efectivo el derecho, y aporte alguno de los siguientes documentos:

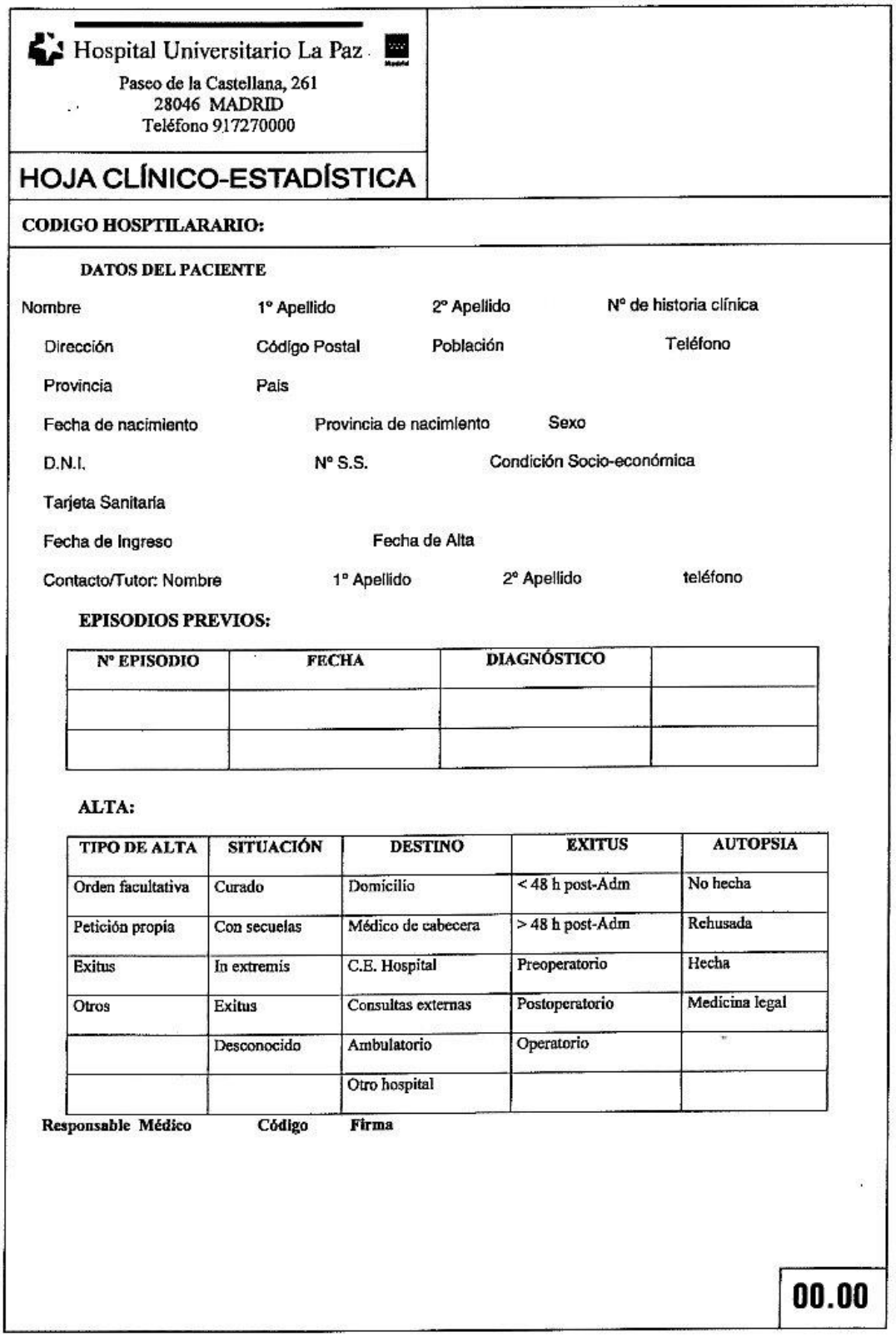
•la negativa del responsable del tratamiento a la oposición de los datos solicitados.

•copia sellada por el responsable del tratamiento del modelo de petición de oposición.

•copia del modelo de solicitud de oposición sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

•cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

Anexo [I] Hoja Clínico-estadística del Hospital Universitario La Paz



Hospital Universitario La Paz

Paseo de la Castellana, 261
28046 MADRID
Teléfono 917270000

HOJA CLÍNICO-ESTADÍSTICA

CODIGO HOSPTILARARIO:

DATOS DEL PACIENTE

Nombre | 1º Apellido | 2º Apellido | Nº de historia clínica

Dirección | Código Postal | Población | Teléfono

Provincia | País

Fecha de nacimiento | Provincia de nacimiento | Sexo

D.N.I. | Nº S.S. | Condición Socio-económica

Tarjeta Sanitaria

Fecha de Ingreso | Fecha de Alta

Contacto/Tutor: Nombre | 1º Apellido | 2º Apellido | teléfono

EPISODIOS PREVIOS:

Nº EPISODIO	FECHA	DIAGNÓSTICO	

ALTA:

TIPO DE ALTA	SITUACIÓN	DESTINO	EXITUS	AUTOPSIA
Orden facultativa	Curado	Domicilio	< 48 h post-Adm	No hecha
Petición propia	Con secuelas	Médico de cabecera	> 48 h post-Adm	Rehusada
Exitus	In extremis	C.E. Hospital	Preoperatorio	Hecha
Otros	Exitus	Consultas externas	Postoperatorio	Medicina legal
	Desconocido	Ambulatorio	Operatorio	
		Otro hospital		

Responsable Médico **Código** **Firma**

HOJA CLÍNICO-ESTADÍSTICA

00.00

Anexo [J] Hoja de autorización de ingreso del Hospital Universitario La Paz

Hospital Universitario La Paz Madrid

HOSPITAL _____

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

Nº Historia Clínica

Nombre _____

1º Apellido _____

2º Apellido _____

Fecha de nacimiento _____/_____/_____ Sexo _____

Registro Movimiento Enfermos:

HOJA DE ORDEN Y AUTORIZACIÓN DE INGRESO

SERVICIO: PLANTA: HABITACIÓN: CAMA Nº:

MOTIVO DEL INGRESO:

PROCEDENCIA INGRESO

URGENCIA ☐

CONSULTA ☐

OTRAS ☐

Facultativo que ordenó el Ingreso

Dr./a.: Firma

Fecha de Ingreso: --------/----------/----------

Cód. 007719

ALTA VOLUNTARIA

AUTORIZACIÓN DEL PACIENTE / FAMILIAR RESPONSABLE

En cumplimiento de la legislación vigente, y el respeto a la autonomía del paciente, le rogamos se sirva firmar la siguiente autorización de ingreso:

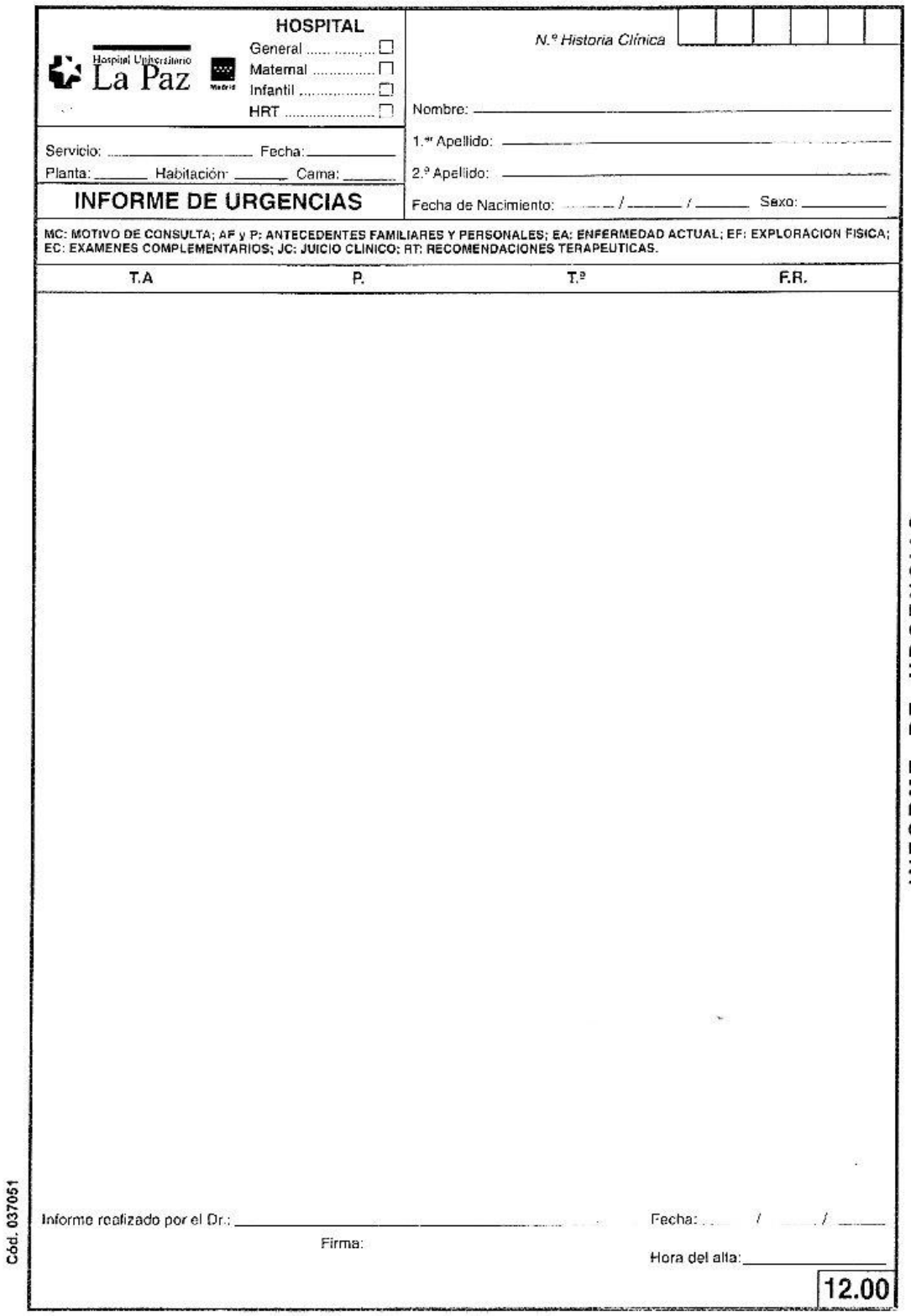
Autorizo mi ingreso hospitalario/ o de mi familiar, por motivos de salud, sin perjuicio de que se requiera nuevamente mi consentimiento para la realización de técnicas diagnósticas o terapéuticas cuando sea necesario.

Mi consentimiento del ingreso es voluntario y conservo el derecho de retirarlo cuando lo considere oportuno.

D./DÑA.
DNI:

09.00

Anexo [K] Informe de Urgencias del Hospital Universitario La Paz



Hospital Universitario La Paz

HOSPITAL
General ..... ☐
Maternal ..... ☐
Infantil ..... ☐
HRT ..... ☐

N.º Historia Clínica

Nombre:

1.er Apellido:

2.º Apellido:

Servicio: Fecha:

Planta: Habitación: Cama:

Fecha de Nacimiento: / / Sexo:

INFORME DE URGENCIAS

MC: MOTIVO DE CONSULTA; AF y P: ANTECEDENTES FAMILIARES Y PERSONALES; EA: ENFERMEDAD ACTUAL; EF: EXPLORACION FISICA; EC: EXAMENES COMPLEMENTARIOS; JC: JUICIO CLINICO; RT: RECOMENDACIONES TERAPEUTICAS.

T.A	P.	T.ª	F.R.

Informe realizado por el Dr.: Fecha: / /

Firma:

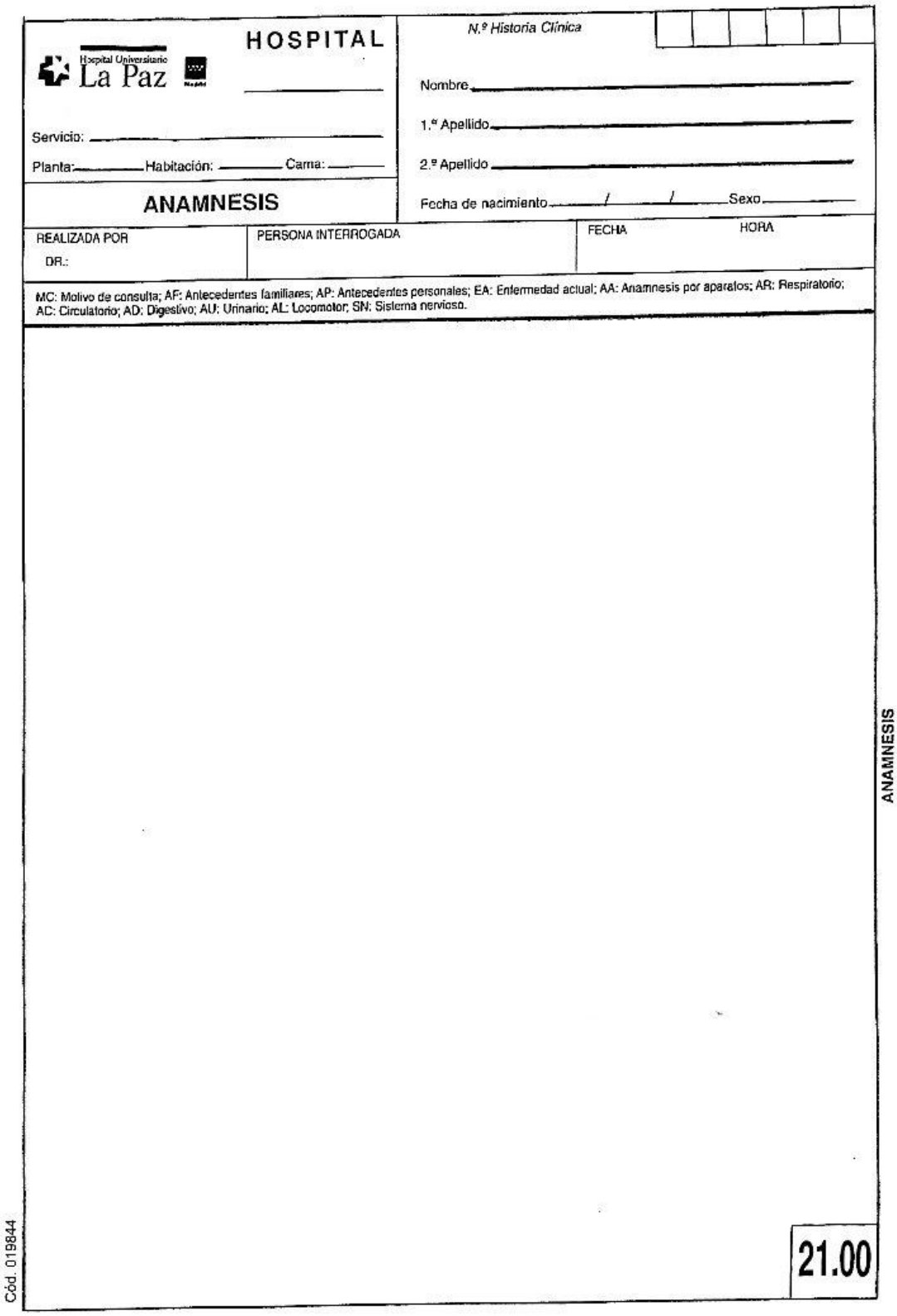
Hora del alta:

12.00

Cód. 037051

INFORME DE URGENCIAS

Anexo L Anamnesis del Hospital Universitario La Paz



HOSPITAL

Hospital Universitario La Paz

Servicio:

Planta: Habitación: Cama:

ANAMNESIS

N.º Historia Clínica

Nombre

1.º Apellido

2.º Apellido

Fecha de nacimiento / / Sexo

REALIZADA POR	PERSONA INTERROGADA	FECHA	HORA
DR.:			

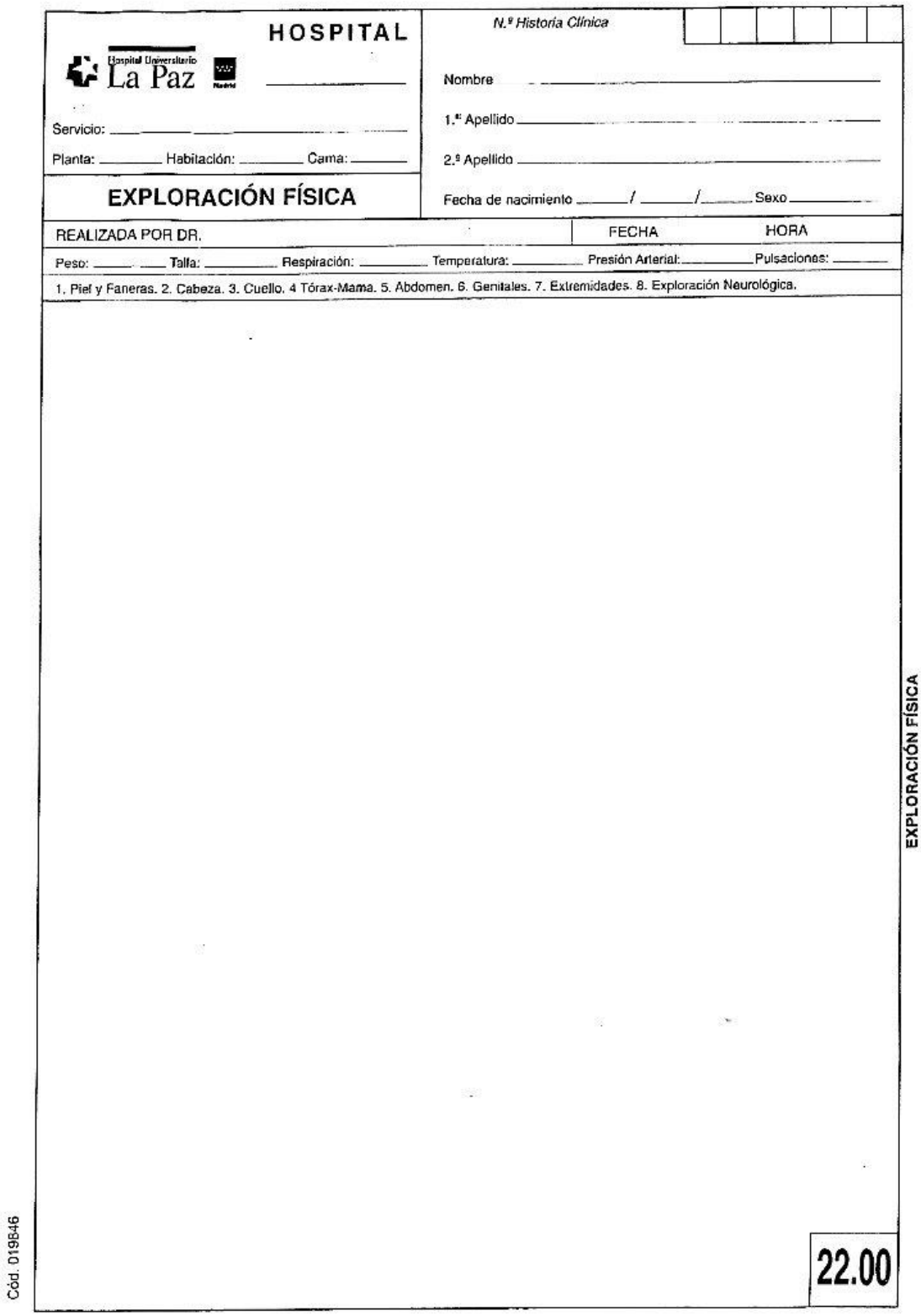
MC: Motivo de consulta; AF: Antecedentes familiares; AP: Antecedentes personales; EA: Enfermedad actual; AA: Anamnesis por aparatos; AR: Respiratorio; AC: Circulatorio; AD: Digestivo; AU: Urinario; AL: Locomotor; SN: Sistema nervioso.

ANAMNESIS

Cód. 019844

21.00

Anexo [M] Hoja de la exploración física del Hospital Universitario La Paz



HOSPITAL

Hospital Universitario La Paz

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

N.º Historia Clínica

Nombre _____

1.er Apellido _____

2.º Apellido _____

Fecha de nacimiento ____/____/____ Sexo _____

EXPLORACIÓN FÍSICA

REALIZADA POR DR. FECHA HORA

Peso: _____ Talla: _____ Respiración: _____ Temperatura: _____ Presión Arterial: _____ Pulsaciones: _____

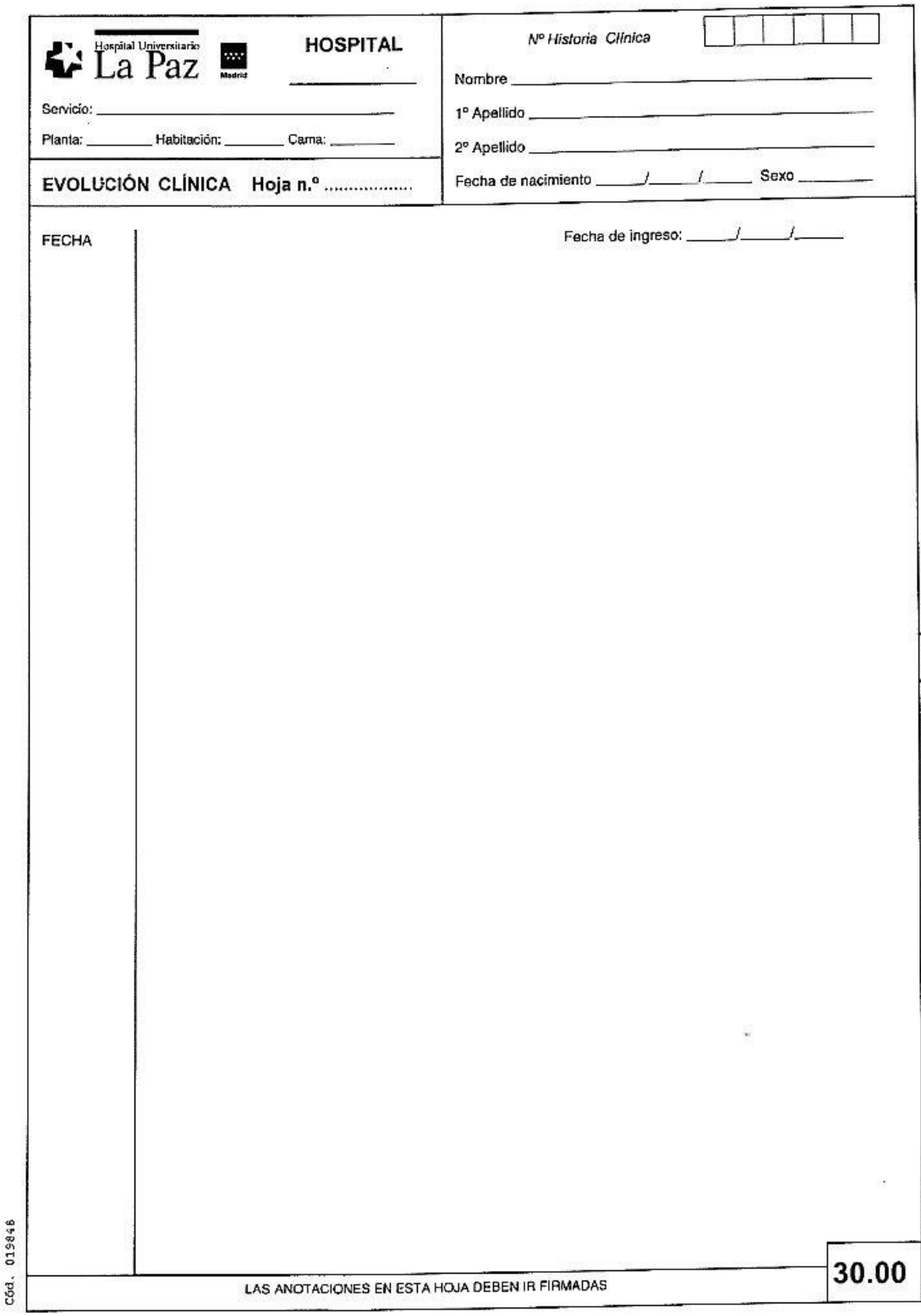
1. Piel y Faneras. 2. Cabeza. 3. Cuello. 4 Tórax-Mama. 5. Abdomen. 6. Genitales. 7. Extremidades. 8. Exploración Neurológica.

EXPLORACIÓN FÍSICA

Cód. 019646

22.00

Anexo [N] Hoja de la evolución del Hospital Universitario La Paz



Hospital Universitario La Paz Madrid

HOSPITAL _____

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

EVOLUCIÓN CLÍNICA Hoja n.º .....

Nº Historia Clínica

Nombre _____

1º Apellido _____

2º Apellido _____

Fecha de nacimiento ____/____/____ Sexo _____

FECHA

Fecha de ingreso: ____/____/____

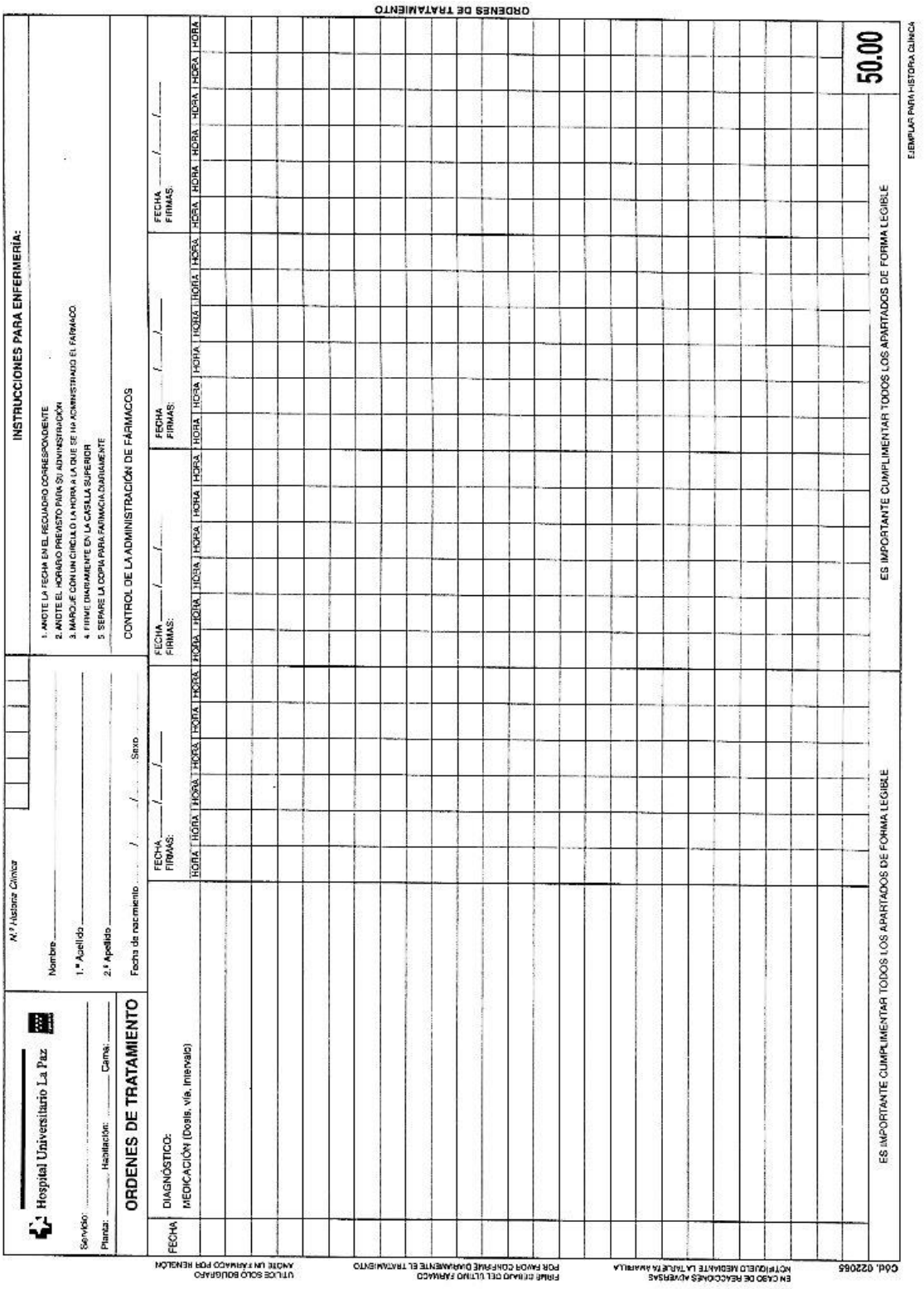
EVOLUCIÓN CLÍNICA

Cód. 019846

LAS ANOTACIONES EN ESTA HOJA DEBEN IR FIRMADAS

30.00

Anexo [O] Hojas de ordenes médicas del Hospital Universitario La Paz



Anexo P Hoja de interconsulta del Hospital Universitario La Paz

Hospital Universitario La Paz

Madrid

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

N.º Historia Clínica

Nombre _____

1.er Apellido _____

2.º Apellido _____

Fecha de nacimiento ____/____/____ Sexo _____

INFORME INTERCONSULTA

FECHA:

SERVICIO CONSULTADO DR.

SERVICIO CONSULTANTE DR.

PRUEBA SOLICITADA:

MOTIVO DE CONSULTA Y DIAGNÓSTICO:

INFORME INTERCONSULTA

Cód. 019852

31.00

Anexo Q Informe de exploraciones complementarias del Hospital Universitario La Paz

Hospital Universitario La Paz

HOSPITAL _____

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

Nº Historia Clínica

Nombre _____

1º Apellido _____

2º Apellido _____

Fecha de nacimiento ____/____/____ Sexo _____

INFORME DE EXPLORACIONES ESPECIALES

FECHA:

SERVICIO CONSULTANTE DR.

SERVICIO CONSULTADO DR.

DIAGNÓSTICO:

MOTIVO DE CONSULTA:

PRUEBA SOLICITADA:

INFORME DE EXPLORACIONES ESPECIALES

Cód. 019854

72.00

Anexo [R] Ejemplo de consentimiento informado Cirugía Plástica del Hospital Universitario la Paz

Hospital Universitario La Paz
SaludMadrid
Comunidad de Madrid

Paseo de la Castellana, 261
28046 MADRID
☎ 91 727 70 00

ETIQUETA
(EN SU DEFECTO, INDIQUE NOMBRE Y UBICACIÓN DEL PACIENTE)

NOMBRE: .....

PROCEDENCIA (CAMA): ..... **NHC :** .....

FECHA : ...../...../..... **GÉNERO :** .....

CONSENTIMIENTO INFORMADO IDENTIFICCACIÓN: T-CPL-002	SERVICIO DE CIRUGÍA PLÁSTICA

BLEFAROPLASTIA

¿QUÉ LE VAMOS A HACER?

1. Descripción del procedimiento

- **En qué consiste:** en eliminar el exceso de piel y músculo de los párpados, tanto superiores como inferiores, así como el tejido graso subyacente. Aunque puede crear un pliegue en el párpado superior de un ojo de tipo asiático, no borrará la evidencia de los rasgos raciales o étnicos.
  Puede realizarse de forma aislada para los párpados superiores, inferiores o ambos, o en combinación con otros procedimientos quirúrgicos sobre ojos, cara, cejas o nariz. La cirugía de los párpados no detiene el proceso de envejecimiento, pero puede disminuir el aspecto de piel flácida y bolsas en la región de los párpados.

- **Cómo se realiza:** mediante incisiones que siguen las líneas naturales de sus párpados: los pliegues de sus párpados superiores y justo por debajo de las pestañas en el párpado inferior. Las incisiones se pueden extender hacia las patas de gallo o líneas que se forman al sonreír en las esquinas exteriores de sus ojos. Trabajando por medio de estas incisiones su cirujano separa la piel de del tejido grasoso interno y del músculo, extrae la grasa excesiva y generalmente corta la piel y músculos caídos. Posteriormente se cierran las incisiones con suturas muy finas. La cirugía del párpado se realiza generalmente bajo anestesia local, junto con sedación oral o intravenosa. Estará despierto durante la cirugía pero se encontrará relajado e insensible al dolor.
  En el curso de la operación pueden surgir condiciones no previstas, que hagan necesario un cambio en lo planeado, siendo necesarios otros tratamientos o la realización de procedimientos como biopsias, radiografías, transfusiones de sangre, etc. Para su realización puede ser necesaria la ayuda de otros especialistas.

- **Cuánto dura:** entre 1 y 3 horas, pudiéndose prolongar en función de los hallazgos intraoperatorios.

2. Qué objetivos persigue:.eliminar el exceso de piel y músculo de los párpados, tanto superiores como inferiores, así como el tejido graso subyacente

¿QUÉ RIESGOS TIENE?

1. Riesgos generales:

Frecuentes y poco graves
- Reacciones alérgicas locales al esparadrapo, material de sutura o preparados tópicos
- Cicatrices anormales (inestéticas o de diferente color al de la piel) o marcas visibles en el párpado o pequeños quistes cutáneos causados por las suturas.
- Problemas de sequedad ocular.
- Sangrado durante o después de la intervención.
- Pérdida de pestañas. en el párpado inferior temporal o permanente.
- Cicatrización retardada (apertura de la herida o retraso en la cicatrización).

Poco frecuentes y graves
- Anestesia local como la general implican un riesgo. Le será facilitada información por el equipo de anestesistas, que recabarán el correspondiente consentimiento escrito.
- Reacciones sistémicas (generales por medicaciones utilizadas durante la cirugía o prescritas posteriormente.
- Lesión de estructuras profundas (nervios, vasos sanguíneos y músculos del ojo) temporal o permanente.
- Infección.
- Asimetría de la cara y/o de la región de los párpados.
- Dolor crónico.
- Ectropion. (separación entre el párpado inferior y el globo ocular)
- Problemas por exposición de la córnea (dificultad en cerrar los párpados, sequedad en la córne).
- Resultado insatisfactorio (deformidades visibles inaceptables, pérdida de la función, apertura de la herida, o pérdida de sensibilidad).

06.00

- - Efectos a largo plazo (alteraciones en el aspecto del párpado como resultado del envejecimiento, pérdida o ganancia de peso, exposición al sol, u otras circunstancias no relacionadas con la cirugía).
- Ceguera es extremadamente rara, puede ser causada por un sangrado interno alrededor del globo ocular durante o después de la cirugía.

2. Riesgos personalizados:

Además de los riesgos anteriormente citados por la/s enfermedad/es que padece puede presentar otras complicaciones..... .

Algunos de estos riesgos son más frecuentes en determinadas condiciones del paciente, por lo que usted debe exponer todos los datos de su historial médico y antecedentes clínico-quirúrgicos, especialmente los referidos a alergias y enfermedades o riesgos personales (ser fumador, hipertensión, etc.....).

La hipertensión que no está bien controlada médicamente puede ser causa de sangrado durante o después de la cirugía. Los acúmulos de sangre bajo los párpados pueden retrasar la curación y causar cicatrización excesiva.

3. Beneficios del procedimiento a corto y medio plazo: disminuir el aspecto de piel flácida y bolsas en la región de los párpados.Mejorar la visión en personas mayores que presentan un exceso importante de párpado superior que cae sobre la pupila

¿QUÉ OTRAS ALTERNATIVAS HAY?

Otros tratamientos o cirugías, como un estiramiento frontal, cuando esté indicado. Otras formas de cirugía de los párpados si existen caída de los párpados por problemas musculares (ptosis palpebral), o laxitud entre el párpado y el globo ocular (ectropion).

¿NOS AUTORIZA?

Por este documento solicitamos su autorización para realizarle la intervención, y usar imágenes e información de su Historia Clínica con fines docentes o científicos, ya que está siendo atendido en un Hospital Universitario. Su anonimato será respetado.

DECLARACIONES Y FIRMAS

Antes de firmar este documento, si desea más información o tiene cualquier duda sobre su enfermedad, no dude en preguntarnos. Le atenderemos con mucho gusto. Le informamos que tiene derecho a revocar su decisión y retirar su consentimiento.

Conforme a lo dispuesto en la LOPD (Ley de Protección de Datos) 15/1999 de 13 de diciembre se informa que sus datos serán objeto de tratamientos e incorporados a ficheros del área 5 Atención especializada con fines asistenciales, de gestión investigación científica y docencia. Solo podrán ser cedidos a organismos autorizados. Podrá ejercer el derecho a acceso, cancelación, rectificación y oposición en la Gerencia del Área.

1.Relativo al paciente:

D./D.ª ..... con D.N.I. ..... .

He sido informado/a suficientemente de la intervención que se me va a realizar, explicándome sus riesgos, complicaciones y alternativas; la he comprendido y he tenido el tiempo suficiente para valorar mi decisión. Por tanto, estoy satisfecho/a con la información recibida. Por ello, doy mi consentimiento para que se me realice dicha intervención por el médico responsable y/o médico residente supervisado por facultativo especialista. Mi aceptación es voluntaria y puedo retirar este consentimiento cuando lo crea oportuno, sin que esta decisión repercuta en mis cuidados posteriores.

Sé que estoy siendo atendido en un Hospital Universitario. Autorizo SI ☐ NO ☐ para utilizar material gráfico o biológico resultado de la intervención con fines docentes y científicos.

Firma del paciente Fecha: ...../...../.....

2. Relativo al médico (cirujano):

Dr./Dra. ..... he informado al paciente y/o al tutor o familiar del objeto y naturaleza de la intervención que se le va a realizar explicándole los riesgos, complicaciones y alternativas posibles.

Firma del médico Fecha: ...../...../.....

3. Relativo a los familiares y tutores:

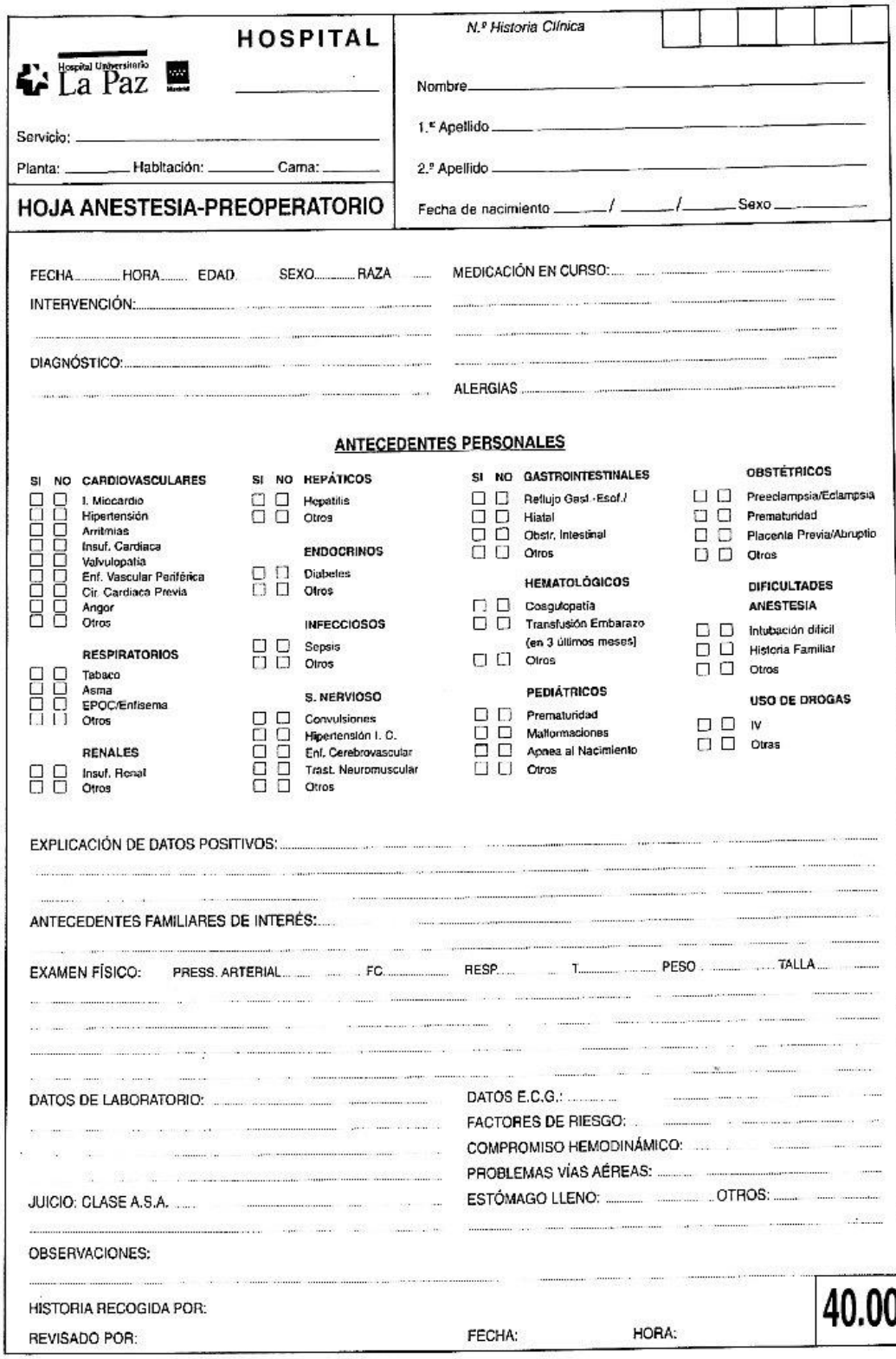
El paciente D./Dña. ..... no tiene capacidad para decidir en este momento.

D./Dª. .... con D.N.I. ..... y en calidad de ..... he sido informado/a suficientemente de la intervención que se le va a realizar. Por ello, doy expresamente mi consentimiento. Mi aceptación es voluntaria y puedo retirar este consentimiento cuando lo crea oportuno.

Firma del tutor o familiar Fecha: ...../...../.....

06.00

Anexo S Informe de Anestesia del Hospital Universitario la Paz



HOSPITAL

Hospital Universitario La Paz

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

N.º Historia Clínica

Nombre _____

1.º Apellido _____

2.º Apellido _____

Fecha de nacimiento ___/___/___ Sexo _____

HOJA ANESTESIA-PREOPERATORIO

FECHA ..... HORA ..... EDAD ..... SEXO ..... RAZA ..... MEDICACIÓN EN CURSO: .....

INTERVENCIÓN: .....

DIAGNÓSTICO: .....

ALERGIAS .....

ANTECEDENTES PERSONALES

SI	NO	CARDIOVASCULARES
☐	☐	I. Miocardio
☐	☐	Hipertensión
☐	☐	Arritmias
☐	☐	Insuf. Cardiaca
☐	☐	Valvulopatía
☐	☐	Enf. Vascular Periférica
☐	☐	Cir. Cardiaca Previa
☐	☐	Angor
☐	☐	Otros

SI	NO	RESPIRATORIOS
☐	☐	Tabaco
☐	☐	Asma
☐	☐	EPOC/Enfisema
☐	☐	Otros

SI	NO	RENALES
☐	☐	Insuf. Renal
☐	☐	Otros

SI	NO	HEPÁTICOS
☐	☐	Hepatitis
☐	☐	Otros

SI	NO	ENDOCRINOS
☐	☐	Diabetes
☐	☐	Otros

SI	NO	INFECCIOSOS
☐	☐	Sepsis
☐	☐	Otros

SI	NO	S. NERVIOSO
☐	☐	Convulsiones
☐	☐	Hipertensión I. C.
☐	☐	Enf. Cerebrovascular
☐	☐	Trast. Neuromuscular
☐	☐	Otros

SI	NO	GASTROINTESTINALES
☐	☐	Reflujo Gast.-Esof./
☐	☐	Hiatal
☐	☐	Obstr. Intestinal
☐	☐	Otros

SI	NO	HEMATOLÓGICOS
☐	☐	Coagulopatía
☐	☐	Transfusión Embarazo (en 3 últimos meses)
☐	☐	Otros

SI	NO	PEDIÁTRICOS
☐	☐	Prematuridad
☐	☐	Malformaciones
☐	☐	Apnea al Nacimiento
☐	☐	Otros

SI	NO	OBSTÉTRICOS
☐	☐	Preeclampsia/Eclampsia
☐	☐	Prematuridad
☐	☐	Placenta Previa/Abruptio
☐	☐	Otros

SI	NO	DIFICULTADES ANESTESIA
☐	☐	Intubación difícil
☐	☐	Historia Familiar
☐	☐	Otros

SI	NO	USO DE DROGAS
☐	☐	IV
☐	☐	Otras

EXPLICACIÓN DE DATOS POSITIVOS: .....

ANTECEDENTES FAMILIARES DE INTERÉS: .....

EXAMEN FÍSICO: PRESS. ARTERIAL ..... FC ..... RESP ..... T ..... PESO ..... TALLA .....

DATOS DE LABORATORIO: .....

DATOS E.C.G.: .....

FACTORES DE RIESGO: .....

COMPROMISO HEMODINÁMICO: .....

PROBLEMAS VÍAS AÉREAS: .....

JUICIO: CLASE A.S.A. .....

ESTÓMAGO LLENO: ..... OTROS: .....

OBSERVACIONES:

HISTORIA RECOGIDA POR:

REVISADO POR: FECHA: HORA:

40.00

Cód. 019834

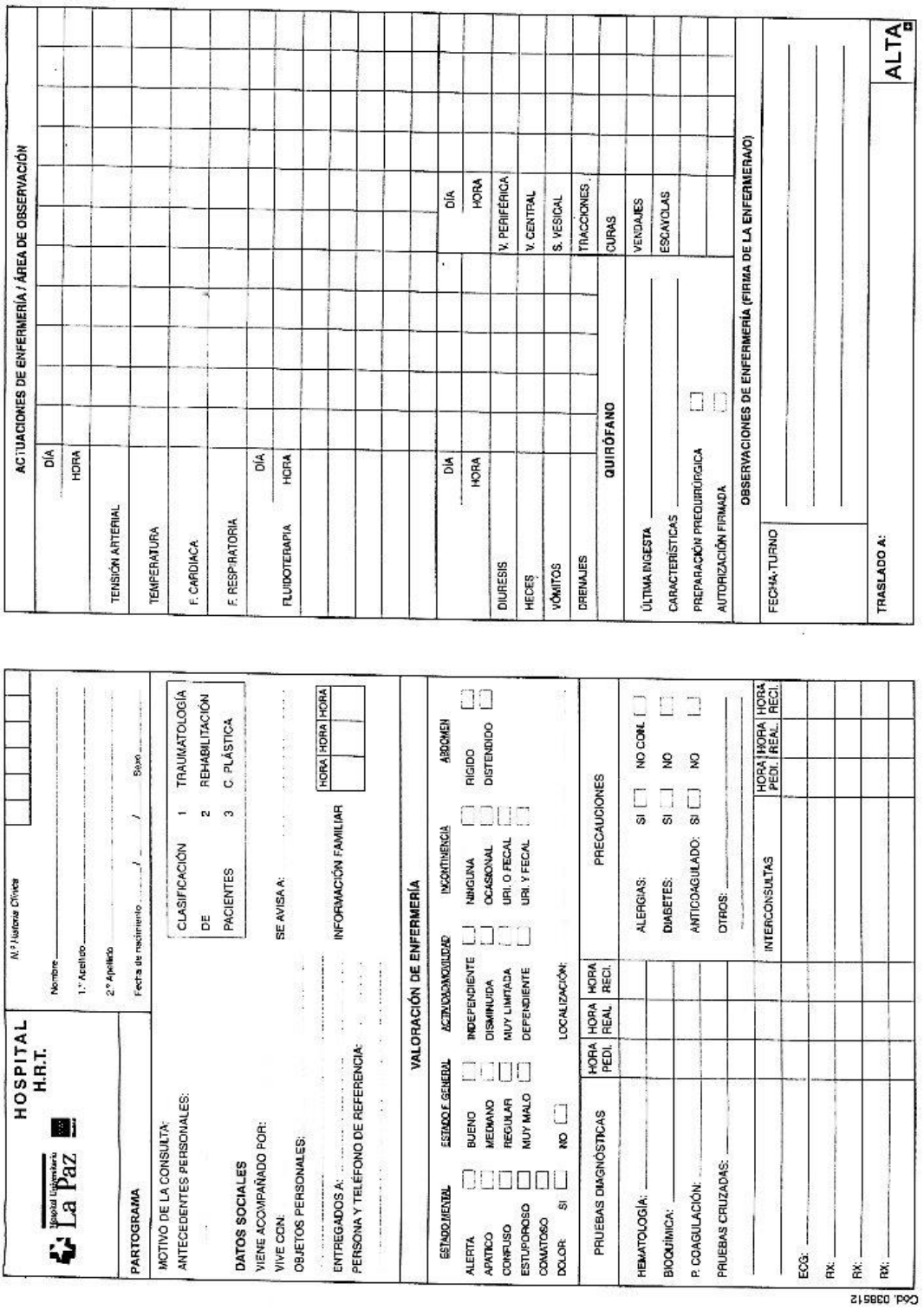
HOJA ANESTESIA-PREOPERATORIO

ESCALA DE GLASGOW		PUNT.
APERTURA DE OJOS	ESPONTANEAMENTE	4
	A LA PALABRA	3
	AL DOLOR	2
	NO	1
RESPUESTA VERBAL	ORIENTADA	5
	CONVERSACIÓN CONFUSA	4
	PALABRAS INAPROPIADAS	3
	SONIDOS INCOMPRENSIBLES	2
	NINGUNA	1
RESPUESTA MOTORA	OBEDECE ORDENES	6
	LOCALIZA DOLOR	5
	RETIRADA AL DOLOR	4
	FLEXIÓN ANORMAL	3
	EXTENSIÓN AL DOLOR	2
	NINGUNA	1
TOTAL		

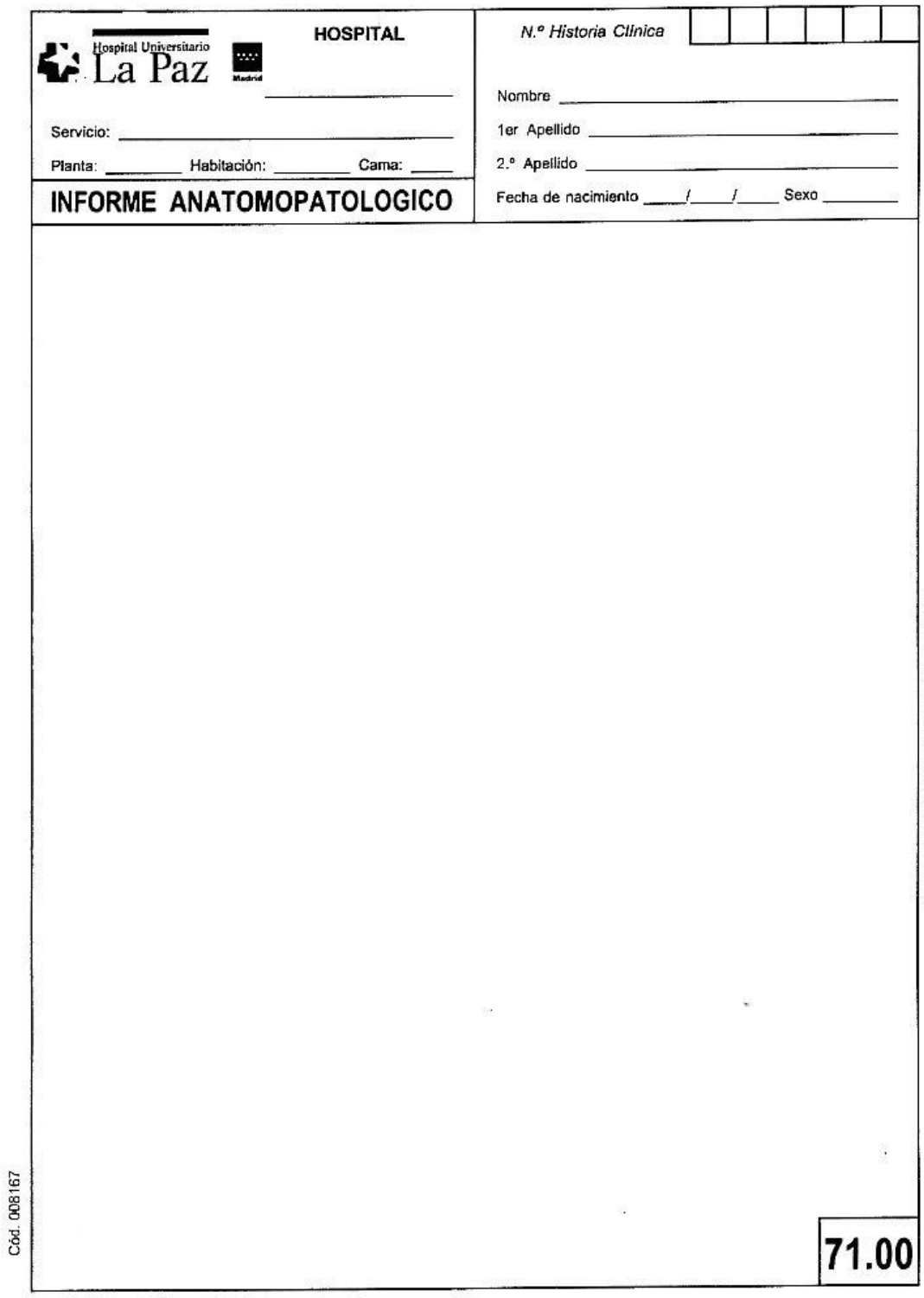
CLASIFICACIÓN A. S. A.
CLASE 1: Paciente sin trastorno orgánico, bioquímico o psiquiátrico. Problema localizado, no entrañando trastorno sistémico.
CLASE 2: Existencia de trastorno sistémico moderado, producido por el problema que origina la intervención o por otros procesos patológicos.
CLASE 3: Existencia de trastorno sistémico severo de cualquier causa.
CLASE 4: Existencia de trastorno severo con amenaza para la vida. No siempre corregible con la intervención.
CLASE 5: Paciente moribundo con escasa probabilidad de supervivencia, sometido a la intervención a la desesperada.
E (OPERACIÓN DE URGENCIA) Intervención urgente en paciente clasificado en cualquiera de los niveles anteriores. Añade un riesgo. Se coloca la letra E detrás de la clase correspondiente.

DATOS ADICIONALES, PRUEBAS COMPLEMENTARIAS ESPECIALES
ANGIOCARDIOGRAFÍA Y HEMODINAMIA
ECOCARDIOGRAFÍA
T.A.C.
ECOGRAFÍA
OTROS
COMENTARIOS DEL EQUIPO ANESTÉSICO

Anexo T Partograma del Hospital Universitario la Paz



Anexo [U] Informe de Anatomía Patológica del Hospital Universitario la Paz



Hospital Universitario La Paz

HOSPITAL _____

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

INFORME ANATOMOPATOLOGICO

N.º Historia Clínica

Nombre _____

1er Apellido _____

2.º Apellido _____

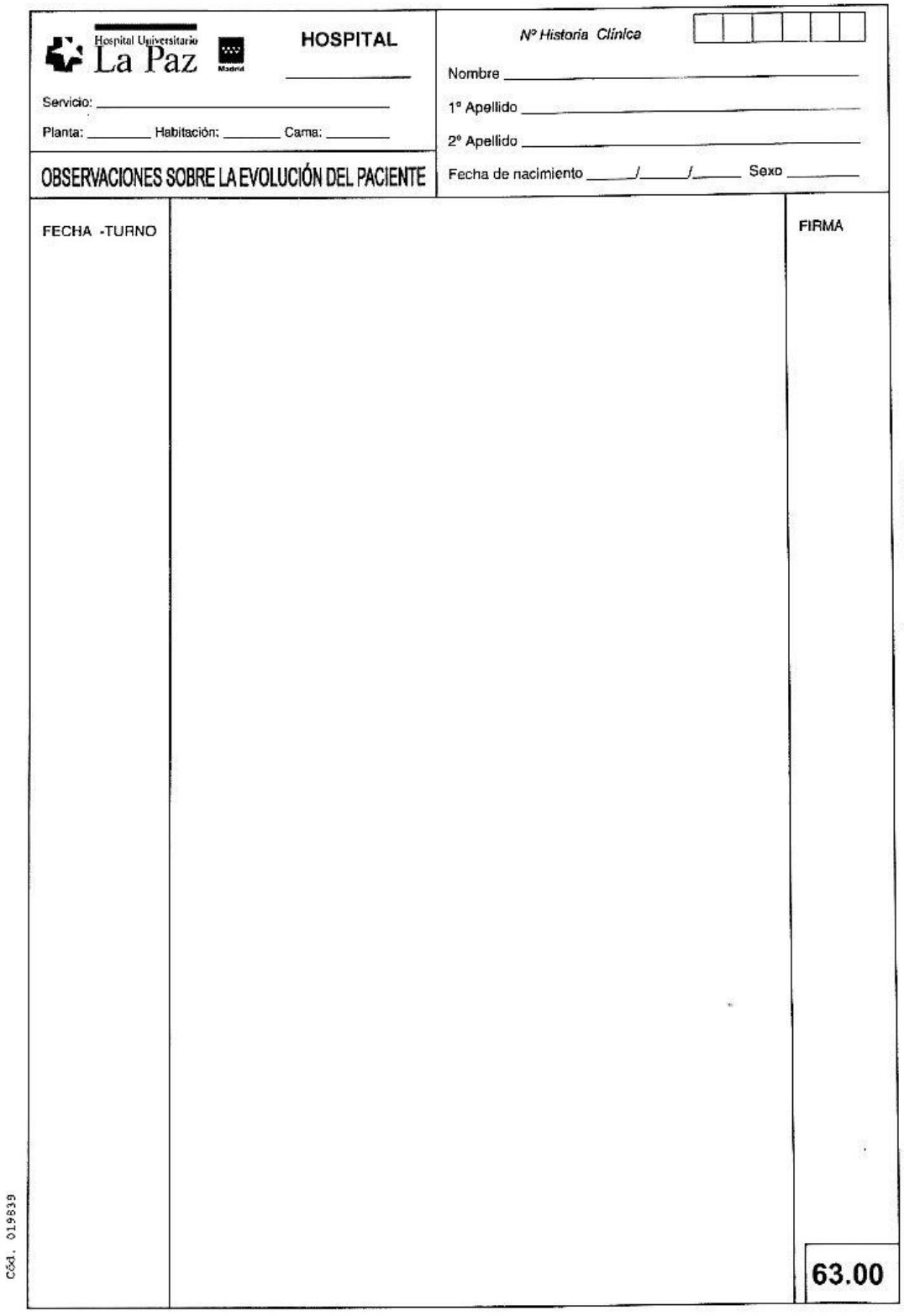
Fecha de nacimiento ____/____/____ Sexo _____

INFORME ANATOMOPATOLOGICO

Cód. 008167

71.00

Anexo V Hoja de observaciones de la Evolución del Paciente por Enfermería del Hospital Universitario la Paz



Hospital Universitario La Paz

HOSPITAL _____

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

Nº Historia Clínica

Nombre _____

1º Apellido _____

2º Apellido _____

Fecha de nacimiento ____/____/____ Sexo _____

OBSERVACIONES SOBRE LA EVOLUCIÓN DEL PACIENTE

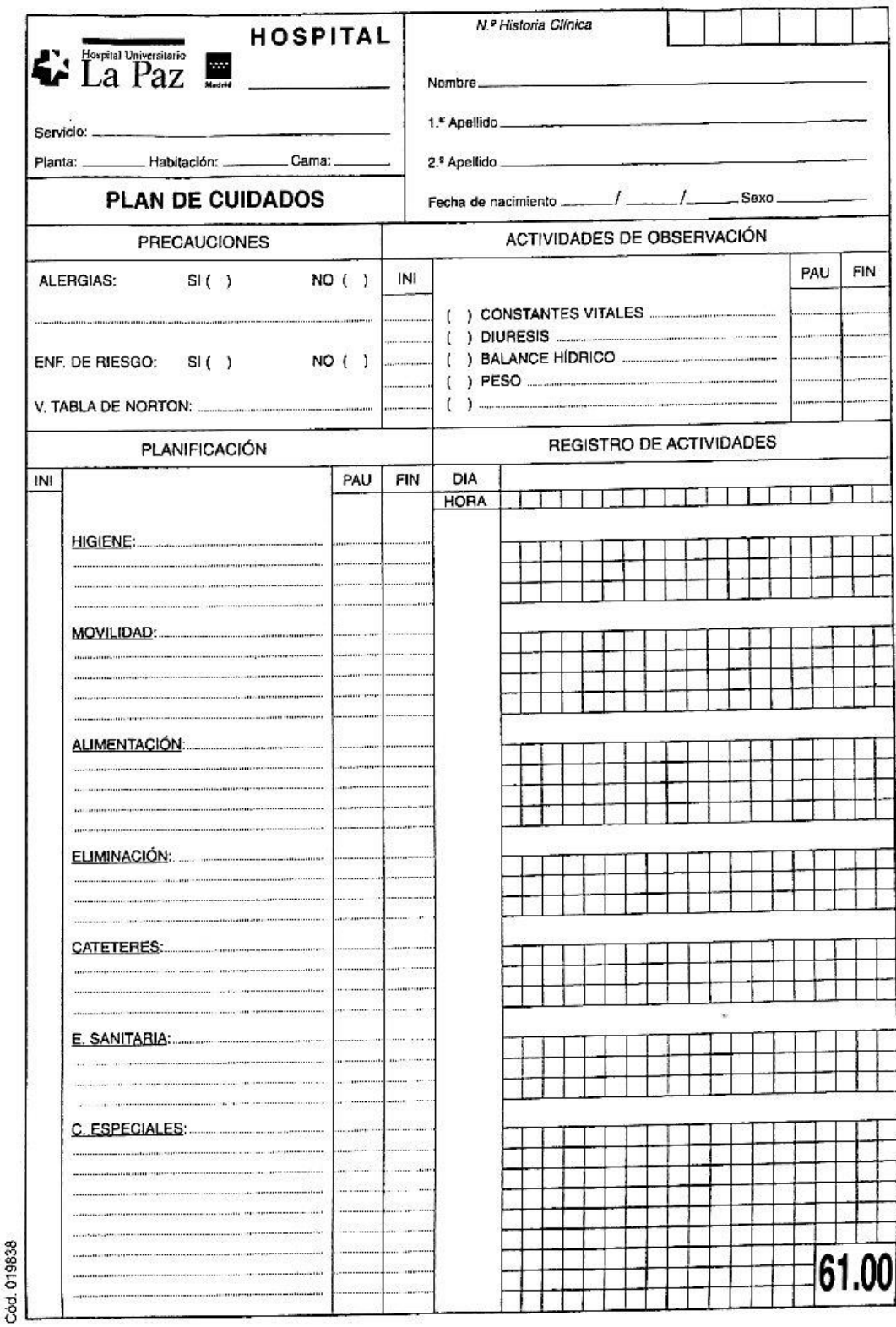
FECHA -TURNO		FIRMA

OBSERVACIONES SOBRE LA EVOLUCIÓN DEL PACIENTE

Cód. 019839

63.00

Anexo [W] Plan de Cuidados del Hospital Universitario la Paz



HOSPITAL Hospital Universitario La Paz Madrid _____

Servicio: _____

Planta: _____ Habitación: _____ Cama: _____

N.º Historia Clínica

Nombre _____

1.º Apellido _____

2.º Apellido _____

Fecha de nacimiento ____/____/____ Sexo _____

PLAN DE CUIDADOS

PRECAUCIONES

ALERGIAS: SI ( ) NO ( )

ENF. DE RIESGO: SI ( ) NO ( )

V. TABLA DE NORTON: _____

ACTIVIDADES DE OBSERVACIÓN

INI		PAU	FIN
	( ) CONSTANTES VITALES		
	( ) DIURESIS		
	( ) BALANCE HÍDRICO		
	( ) PESO		
	( )		

PLANIFICACIÓN

INI		PAU	FIN
	HIGIENE:		
	MOVILIDAD:		
	ALIMENTACIÓN:		
	ELIMINACIÓN:		
	CATETERES:		
	E. SANITARIA:		
	C. ESPECIALES:		

REGISTRO DE ACTIVIDADES

DIA

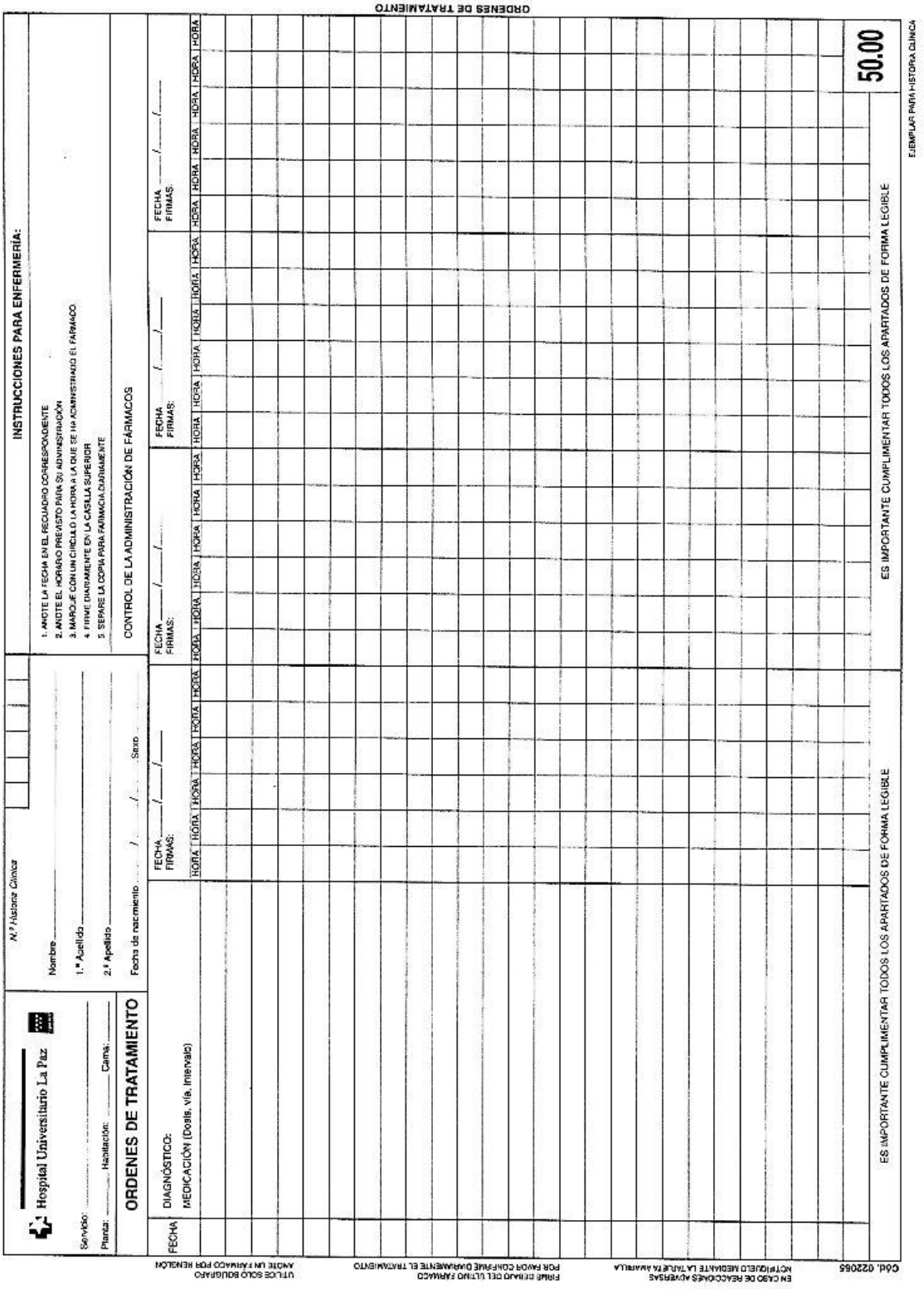
HORA

PLAN DE CUIDADOS

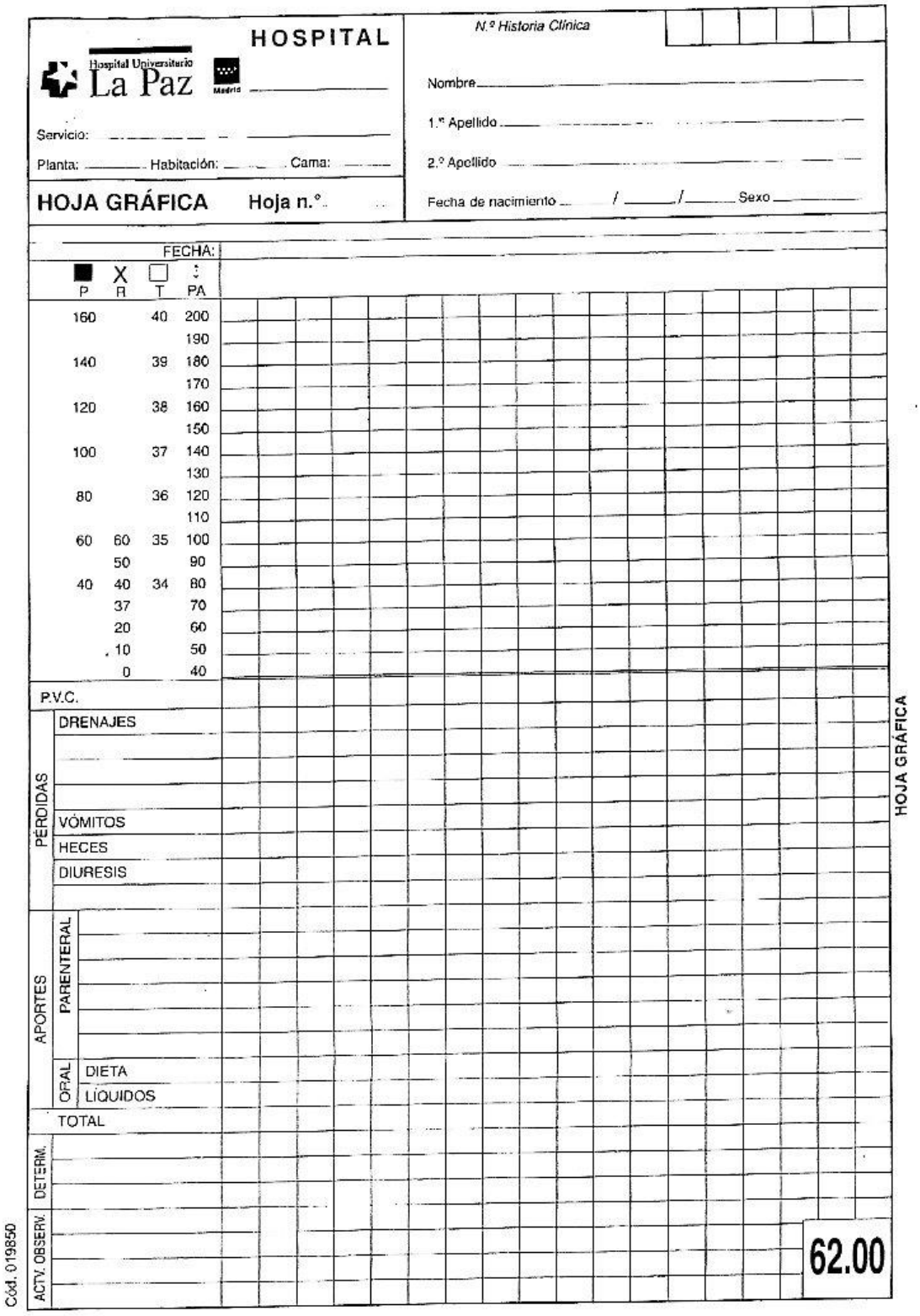
Cód. 019838

61.00

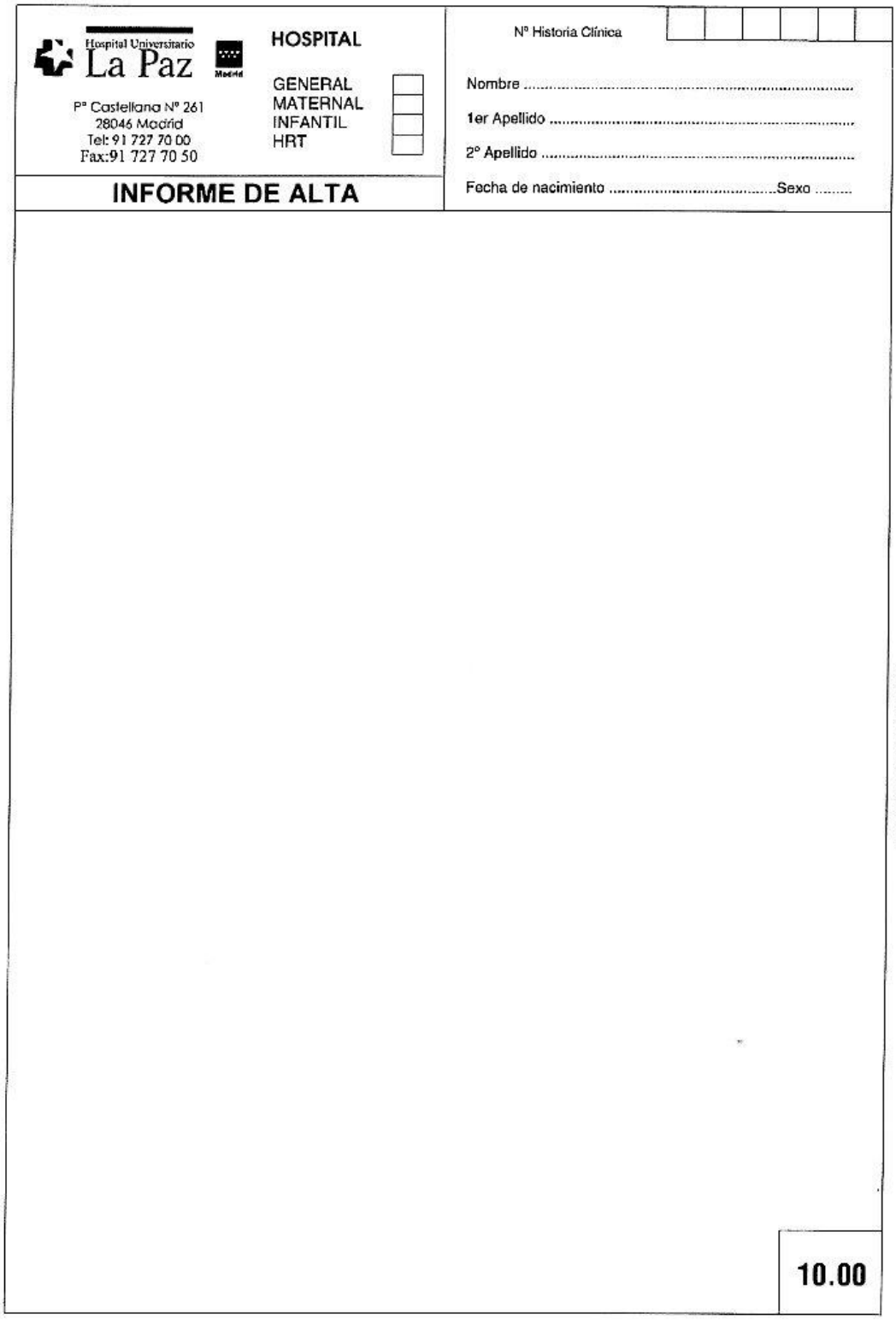
Anexo [X] Hoja de Orden de tratamiento del Hospital Universitario la Paz



Anexo [Y] Hoja Gráfica del Hospital Universitario la Paz



Anexo [Z] Informe de Alta del Hospital Universitario la Paz



Hospital Universitario La Paz

Madrid

Pº Castellana Nº 261
28046 Madrid
Tel: 91 727 70 00
Fax:91 727 70 50

HOSPITAL

GENERAL ☐
MATERNAL ☐
INFANTIL ☐
HRT ☐

Nº Historia Clínica

Nombre .....

1er Apellido .....

2º Apellido .....

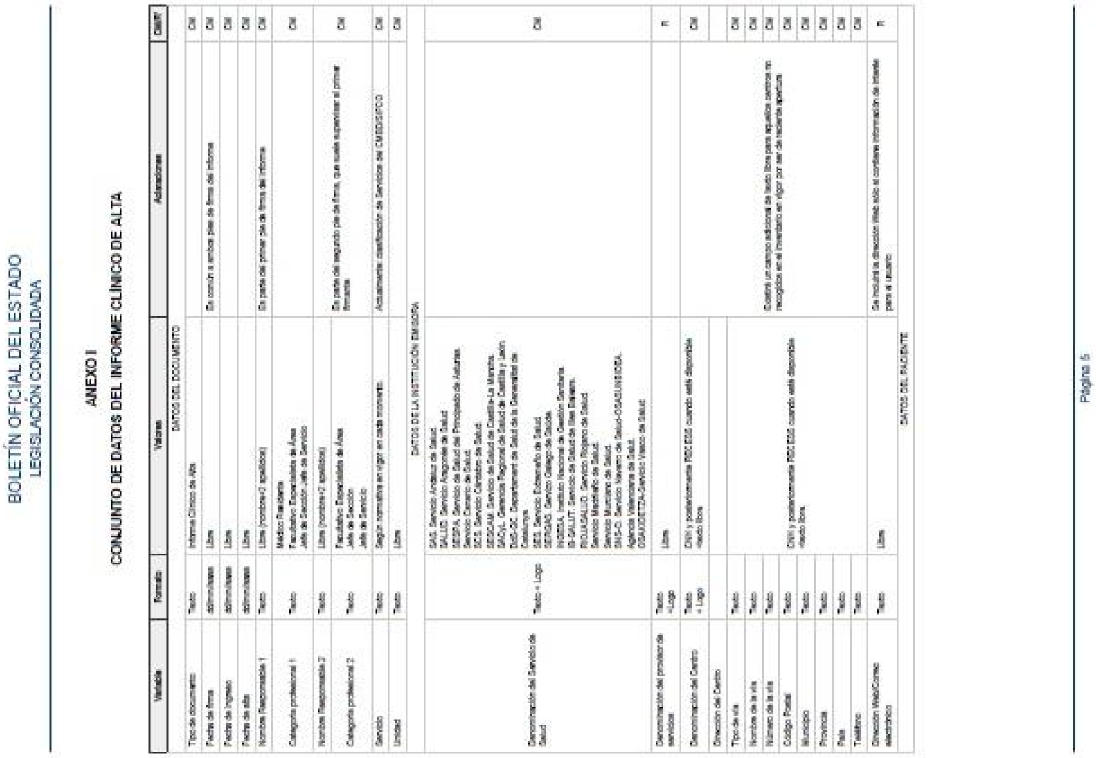
Fecha de nacimiento .....Sexo .....

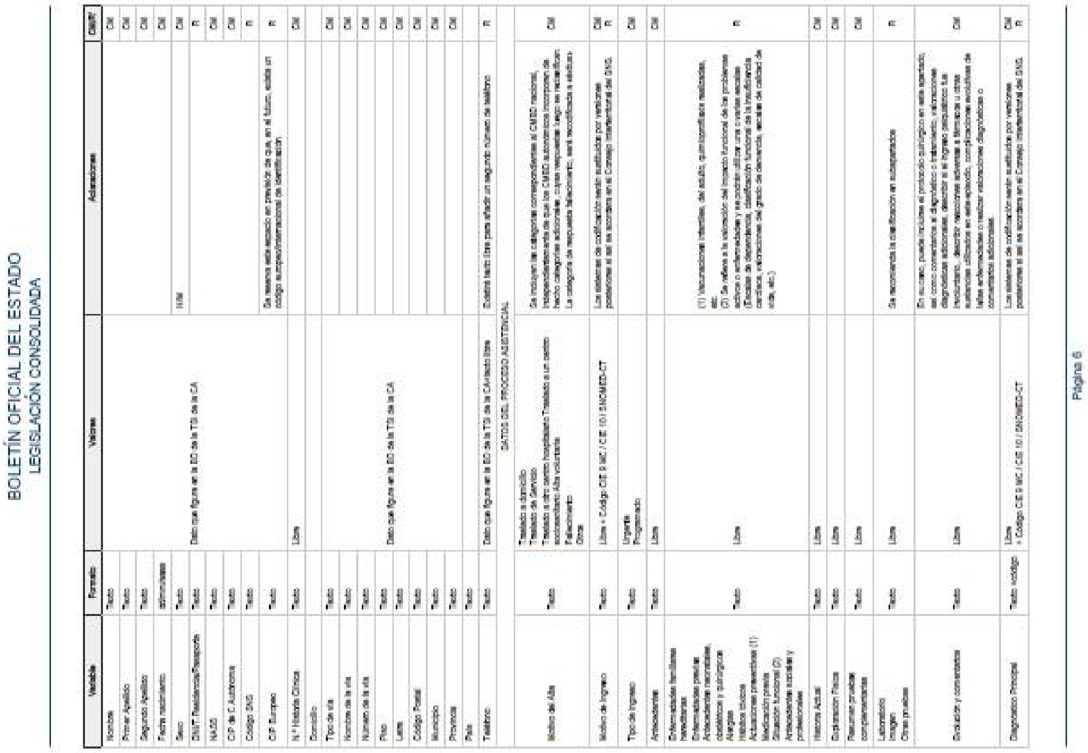
INFORME DE ALTA

INFORME DE ALTA

10.00

Anxo AA Conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud





Variable	Formato	Valores	Aclaraciones	CM/R*
Otros Diagnósticos	Texto =código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM/ R
Procedimientos	Texto =código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM/ R
Tratamiento	Texto	Libre		CM
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyan fármacos (cotgerciancia, dieta, reposo o limitaciones de esfuerzo físico, etc.)	R
Fármacos	Texto =código	Libre (Especialidad + principio activo + dosis/unidad+ nº unidades/dosis+ Intervalo de dosis+ vía administración+ duración) nomenclador oficial MSPS (código nacional)/Snomed-CT	En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyan módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclador Oficial/ Snomed-CT)	R
Otras Recomendaciones	Texto	Libre	Se refiere a los planes de actuación previstos que no son propiamente medidas terapéuticas. Por ejemplo, fecha de próxima cita, conveniencia de nueva revisión, petición de pruebas, etc.	CM

* Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

ANEXO II

CONJUNTO DE DATOS DEL INFORME CLÍNICO DE CONSULTA EXTERNA

Variable	Formato	Valores	Aclaraciones	CM/R*
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe Clínico de Consulta Externa		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	CM
Fecha de Consulta	dd/mm/aaaa	Libre		CM
Nombre Responsable 1	Texto	Libre (nombre+2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional 1	Texto	Médico Residente Facultativo Especialista de Área Jefe de Sección Jefe de Servicio		CM
Nombre Responsable 2	Texto	Libre (nombre+2 apellidos)	Es parte del segundo pie de firma, que suele supervisar al primer firmante	CM
Categoría profesional 2	Texto	Facultativo Especialista de Área Jefe de Sección Jefe de Servicio		CM
Servicio	Texto	Según normativa en vigor en cada momento	Actualmente: clasificación de Servicios del CMBD/SIPCO	CM
Unidad	Texto	Libre		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud. SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud. SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL. Gerencia Regional de Salud de Castilla y León. DoS-DC. Departament de Salut de la Generalitat de Catalunya. SES. Servicio Extremeño de Salud. SERGAS. Servicio Gallego de Salcide. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears.		CM
		RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud. SNS-O. Servicio Navarro de SaludOSASUNBIDEA. Agéncia Valenciana de Salut. OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del proveor de servicios	Texto + Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible +texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura.	CM

Variable	Formato	Valores	Aclaraciones	CM/R*
Dirección del centro				
Tipo de vía	Texto	CNH y posteriormente RECESS cuando esté disponible +texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura.	CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto	Dato que figure en la BD de la TSI de la CA	H/M	CM
DNI/ Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de C.Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación.	R
N.º Historia Clínica	Texto	Libre		CM
Domicilio				
Tipo de vía	Texto	Dato que figure en la BD de la TSI de la CA		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			
Teléfono	Texto	Dato que figure en la BD de la TSI de la CA+texto libre	Existirá texto libre para añadir un segundo número de teléfono	R
DATOS DEL PROCESO ASISTENCIAL				
Motivo de Consulta	Texto =código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM/ R
Antecedentes	Texto	Libre	Se recomienda la clasificación en subapartados	CM
Enfermedades familiares hereditarias Enfermedades previas Antecedentes Neonatales, Quirúrgicos y Ginecológicos Alergias Hábitos tóxicos Actuaciones Preventivas (1) Medicación previa			(1) Vacunaciones infantiles, del adulto, quimioprofilaxis realizadas, etc. (2) Se refiere a la valoración del impacto funcional de los problemas activos o enfermedades y se podrán utilizar una o varias escalas (Escalas de dependencia, clasificación	R
Situación funcional (2) Antecedentes sociales y profesionales			funcional de la insuficiencia cardiaca, Valoraciones del grado de dependencia, Escalas de Calidad de vida, etc.)	
Historia Actual	Texto	Libre		CM
Exploración Física	Texto	Libre		CM
Resumen pruebas complementarias	Texto	Libre		CM
Laboratorio Imagen Otras pruebas	Texto	Libre	Se recomienda la clasificación en subapartados	R

Variable	Formato	Valores	Aclaraciones	CMI/R[1]
Evolución y comentarios	Texto	Libre	Se pueden realizar comentarios del seguimiento evolutivo, en el caso de que el informe no se refiera a una sola consulta sino a un periodo de seguimiento en el que se han realizado varias entrevistas clínicas. En este caso se puede incluir aquí el periodo de tiempo del que se comprenativo el informe o reseñar las fechas en las que se produjeron las consultas. También es el lugar adecuado para describir reacciones adversas a fármacos utilizados en este episodio o describir complicaciones evolutivas de la/las enfermedades, realizar valoraciones diagnósticas o comentarios adicionales	CM
Diagnóstico Principal	Texto +código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Otros Diagnósticos	Texto +código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Procedimientos	Texto +código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Tratamiento	Texto	Libre		CM
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyan fármacos (psicoterapia, dieta, reposo o limitaciones de esfuerzo físico, etc.)	R
Fármacos	Texto +código	Libre (Especialidad+principio activo+ dosis/unidad+ n.º unidades/dosis+ intervalo de dosis+ v/a administración + duración) nomenclator oficial MSPS (código nacional)/Snomed-CT	Prescripciones activas al final del periodo de seguimiento. En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyan módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclator Oficial/ Snomed-CT).	R
Otras recomendaciones	Texto	Libre	Se refiere a los planes de actuación previstos que no son propiamente medidas terapéuticas. Por ejemplo: fecha de próxima cita, conveniencia de nueva revisión, petición de pruebas, etc.	CM

[1] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

ANEXO III

CONJUNTO DE DATOS DEL INFORME CLÍNICO DE URGENCIAS

Variable	Formato	Valores de referencia	Aclaraciones	CMI/R[1]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe Clínico de Urgencias		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe.	R
Fecha y hora de ingreso o de activación del recurso	dd/mm/aaaa hh:mm	Libre		CM
Fecha y hora de alta	dd/mm/aaaa hh:mm	Libre		CM
Nombre Responsable 1	Texto	Libre (nombre + 2 apellidos)	Es parte del primer pie de firma del informe.	CM
Categoría profesional 1	Texto	Médico Residente Facultativo Jefe de Sección Jefe de Servicio		CM
Nombre Responsable 2		Libre (nombre + 2 apellidos)	Es parte del segundo pie de firma, que suele supervisar el primer firmante.	CM
Categoría responsable 2		Facultativo Jefe de Sección Jefe de Servicio		CM
Unidad Asistencial responsable	Texto	Servicio de Urgencia Hospitalaria Servicio de Urgencia de A.Primaria SAMU S.º Urgencias + texto libre		CM
DATOS DE LA INSTITUCIÓN EMISORA				

Variable	Formato	Valores de referencia	Aclaraciones	CMI/R[1]
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud. SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud. SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL. Gerencia Regional de Salud de Castilla y León. DoS-GC. Departament de Salut de la Generalitat de Catalunya. SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Baleares. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud. SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agència Valenciana de Salut. OSAKIDETZA-Servicio Vasco de Salud.		CM
Denominación del proveor de servicios	Texto +logo	Libre		R
Denominación del Centro	Texto + Logo	CNH para Centros de Atención Especializada. Inventario para Centros de Primaria RECESS para ambos cuando esté disponible +texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura.	CM
Dirección del Centro				
Tipo de vía	Texto			CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo Electrónico	Texto		Se incluirá la dirección Web sólo si contiene información de interés para el usuario.	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha de nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T. Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de la C. Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo			Se reserva este espacio en previsión de que en el futuro exista un código europeo/internacional de identificación.	R
N.º Historia Clínica	Texto	Libre		R
Domicilio				
Tipo de vía	Texto	Dato que figure en la BD de TSI de la CA		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			
Teléfono	Texto			R
Persona de Referencia	Texto	Libre (nombre + 2 apellidos)		R
Teléfono de Referencia	Texto	Libre		R
DATOS DEL PROCESO ASISTENCIAL				

Variable	Formato	Valores de referencia	Aclaraciones	CMI/R[1]
Procedencia	Texto	Médico de Familia/Pediatra de AP Por decisión del paciente o familiar Cuerpos de Seguridad Otros Servicios de Urgencias		R
Tipo de Consulta	Texto	Enfermedad Accidente de tráfico Accidente Laboral Otros Accidentes		R
Motivo de Alta	Texto	Ingreso Traslado a domicilio Traslado de Servicio Traslado a otro centro hospitalario Traslado a un centro sociosanitario Alta voluntaria Fallecimiento Otros	Se incluyen aquellas categorías correspondientes al CMBD nacional, independientemente de que los CMBD autonómicos incorporen categorías adicionales cuyas respuestas luego se reclasifican. La categoría de respuesta fallecimiento, será recodificada a exitus	CMI
Motivo de Consulta	Texto + código	Libre + Código CIE 9 MC / CIE 10 / SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CMI R
Antecedentes	Texto	Libre		CMI
Enfermedades Previas Antecedentes neonatales, obstétricos y quirúrgicos Medicación previa Alergias Situación funcional (1) Antecedentes sociales y profesionales	Texto	Libre	(1) Se refiere a la valoración del impacto funcional de los problemas activos o enfermedades, y se podrán utilizar una o varias escalas (Escalas de dependencia, clasificación funcional de la insuficiencia cardiaca, valoraciones del grado de demencia, escalas de calidad de vida, etc.).	R
Historia Actual	Texto	Libre		CMI
Exploración física				CMI
TA (/) FC ( )ppl/min FR ( ) resp/min Temp. ( )ºC Saturación O_2 Glucemia capilar Resumen de exploración	Texto	Libre		R
Resumen de pruebas complementarias	Texto	Libre	Se recomienda la clasificación en subapartados.	CMI
Laboratorio Imagen Otras pruebas	Texto	Libre		R
Evolución y comentarios	Texto	Libre	En su caso pueden incluirse, además de comentarios evolutivos y del período de observación, la descripción de técnicas realizadas durante el proceso de atención. También es el lugar adecuado para describir reacciones adversas a fármacos utilizados en este episodio, complicaciones evolutivas de leñas enfermedades, realizar valoraciones diagnósticas o comentarios adicionales.	CMI
Diagnóstico principal	Texto +código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CMI R
Otros diagnósticos	Texto +código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CMI R
Procedimientos	Texto +código	Libre Código CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CMI R
Tratamiento	Texto	Libre		CMI
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyen fármacos (oxigenoterapia, dieta, reposo o limitaciones de esfuerzo físico, etc.).	R
Fármacos	Texto +código	Libre (Especialidad+principio activo+ dosis/unidad+ n.º unidades/dosis+ intervalo de dosis+ vía administración+ duración) nomenclador oficial MSPS (código nacional)/Snomed-CT	Prescripciones activas. En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyen módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclador Oficial Snomed-CT).	R
Otras recomendaciones	Texto	Libre	Se refiere a los planes de actuación previstos que no son propiamente medidas terapéuticas. Por ejemplo: fecha de próxima cita, conveniencia de nueva revisión, petición de pruebas, etc.	CMI

[1] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

ANEXO IV

CONJUNTO DE DATOS DEL INFORME CLÍNICO DE ATENCIÓN PRIMARIA

Variable	Formato	Valores	Aclaraciones	CMI/R[1]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe Clínico de Atención Primaria		CMI
Fecha de firma	dd/mm/aaaa	Libre	Fecha en la cual se emite el informe. Es común a ambos pies de firma.	CMI
Fecha inicio periodo	dd/mm/aaaa	Libre	Fecha en la que se inicia el periodo de seguimiento en el que se inscriben los diferentes episodios y actuaciones que se describen.	CMI
Fecha fin periodo	dd/mm/aaaa	Libre	Fecha en la que finaliza el periodo de seguimiento en el que se inscriben los diferentes episodios y actuaciones que se describen.	CMI
Nombre Responsable 1	Texto	Libre (nombre + 2 apellidos)		CMI
Categoría profesional 1	Texto	Médico Residente Médico de Familia Pediatra de AP Texto Libre	En parte del primer pie de firma del informe.	CMI
Nombre Responsable 2	Texto	Libre (nombre + 2 apellidos)		CMI
Categoría responsable 2	Texto	Médico de Familia Pediatra de AP Texto Libre	En parte del segundo pie de firma, que suele supervisar el primer firmante.	CMI
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud. SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud. SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL. Gerencia Regional de Salud de Castilla y León. CatSalut. Departament de Salut de la Generalitat de Catalunya. SES. Servicio Extremeño de Salud. SERGAS. Servizo Galego de Saúde. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud. SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agencia Valenciana de Salud. OSAKIDETZA-Servicio Vasco de Salud.		CMI
Denominación del proveedor de servicios	Texto +logo	Libre		R
Denominación del Centro	Texto + Logo	Inventario de Centros de Atención Primaria y posteriormente RECESS cuando esté disponible + texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura.	CMI
Dirección del Centro				
Tipo de vía	Texto	Inventario de Centros de Atención Primaria y posteriormente RECESS cuando esté disponible + texto libre		CMI
Nombre de la vía	Texto			CMI
Número de la vía	Texto			CMI
Piso	Texto			CMI
Letra	Texto			CMI
Código Postal	Texto			CMI
Municipio	Texto			CMI
Provincia	Texto			CMI
País	Texto			CMI
Teléfono	Texto			CMI
Dirección Web/Correo Electrónico	Texto	Libre	Se incluirá la dirección Web ado si contiene información de interés para el usuario.	R
DATOS DEL USUARIO/PACIENTE				

Variable	Formato	Valores	Aclaraciones	CM/R*
Nombre	Texto	Dato que figure en BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha de nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T. Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de la C. Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo			Se reserva este espacio en previsión de que en el futuro, exista un código europeo/internacional de identificación.	R
N.º Historia Clínica	Texto	Libre		CM
Domicilio				
Tipo de vía	Texto	Dato que figure en la BD de TSI de la CA		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			
Teléfono	Texto			R
Persona de Referencia	Texto	Libre (nombre + 2 apellidos)	Se trata de la persona que representa los intereses del paciente.	R
Teléfono de Referencia	Texto	Libre		R
DATOS DE SALUD				
Antecedentes	Texto	Libre	Se recomienda su clasificación en subapartados.	CM
Enfermedades familiares hereditarias Enfermedades previas Antecedentes necrobiales, obstétricos y quirúrgicos Alergias Hábitos tóxicos Actuaciones preventivas (1) Medicación previa Situación funcional (2) Antecedentes sociales y profesionales			(1) Vacunaciones infantiles, del adulto, quimioprofilaxis realizadas, etc. (2) Se refiere a la valoración del impacto funcional de los problemas activos o enfermedades y se podrán utilizar una o varias escalas (Escalas de dependencia, clasificación funcional de la insuficiencia cardíaca, valoraciones del grado de demencia, escalas de calidad de vida, etc.).	R
Resumen pruebas complementarias	Texto	Libre		CM
Laboratorio Imagen Otras pruebas	Texto	Libre	Se recomienda la clasificación en subapartados.	R
Resumen de Episodios Atendidos	Texto + código	Libre Código: CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Evolución y comentarios	Texto	Libre	Se pueden realizar comentarios del seguimiento evolutivo. También es el lugar adecuado para describir reacciones adversas a fármacos utilizados o describir complicaciones evolutivas de la/las enfermedades, realizar valoraciones diagnósticas o comentarios adicionales.	CM
Diagnósticos	Texto + código	Libre Código: CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Procedimientos	Texto + código	Libre Código: CIE 9 MC/CIE 10/CIAP2 definida/SNOMED-CT	Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS.	CM R
Tratamiento	Texto	Libre	Se refiere al último tratamiento que está activo.	CM
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyen fármacos (colgarcolarapia, dieta, reposo o limitaciones de esfuerzo físico, etc.).	R

Variable	Formato	Valores	Aclaraciones	CM/R*
Fármacos	Texto +código	Libre ([Especialidad>principio activo> dosis/unidad> n.º unidades/dosis> intervalo de dosis> vía administración> duración] nomenclator oficial MSPS (código nacional)/Snomed- CT	Prescripciones activas al final del período de seguimiento. En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyen módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclator Oficial/ Snomed-CT).	CM R
Otras Recomendaciones	Texto	Libre	Se refiere a los planes de actuación previstos que no son propiamente medidas terapéuticas. Por ejemplo: fecha de próxima cita, conveniencia de una nueva revisión, petición de pruebas, etc...	R

*Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R)

ANEXO V

CONJUNTO DE DATOS DEL INFORME DE RESULTADOS DE PRUEBAS DE LABORATORIO

Variable	Formato	Valores	Aclaraciones	CM/R*
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe de Resultados de Pruebas de Laboratorio		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies del informe	CM
Nombre Responsable 1	Texto	Libre (nombre+2 apellidos)		CM
Categorías profesional 1	Texto	Médico Residente		CM
		Facultativo Especialista de Área	Es parte del primer pie de firma del informe	
		Farmacéutico Residente		
		Biólogo Residente		
		Jefe de Sección		
		Jefe de Servicio		
		Texto libre		
Nombre Responsable 2	Texto	Libre (nombre+2 apellidos)		CM
Categorías profesional 2	Texto	Facultativo Especialista de Área		CM
		Jefe de Sección	Es parte del segundo pie de firma, que suele supervisar el primer firmante	
		Jefe de Servicio		
		Texto libre		
Servicio	Texto	Análisis Clínicos	RD 1277/2003 y normativa en vigor en cada momento	CM
		Anatomía Patológica		
		Bioquímica Clínica		
		Hematología y Hemoterapia		
		Genética		
		Inmunología		
		Microbiología y parasitología		
Unidad	Texto	Libre		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud.		CM
		SALUD. Servicio Aragonés de Salud		
		SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud		
		SCS. Servicio Cántabro de Salud.		
		SESCAM. Servicio de Salud de Castilla-La Mancha.		
		SACyL. Gerencia Regional de Salud de Castilla y León.		
		DoS-GC. Departament de Salut de la Generalitat de Catalunya		
		SES. Servicio Extremeño de Salud.		
		SERGAS. Servizo Galego de Saúde.		

Variable	Formato	Valores	Aclaraciones	Cl/I/F
		INGESA. Instituto Nacional de Gestión Sanitaria.		
		IB-SALUT. Servicio de Salud de Illes Baleares.		
		RIOJASALUD. Servicio Riojano de Salud.		
		Servicio Madrileño de Salud.		
		Servicio Murciano de Salud.		
		SNS-O. Servicio Navarro de Salud-OSASUNBIDEA.		
		Agència Valenciana de Salut.		
		OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del proveedor de servicios	Texto + Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible + texto libre		CM
Dirección del Centro			Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	
Tipo de Vía	Texto	CNH y posteriormente RECESS cuando esté disponible + texto libre		CM
Nombre de vía	Texto			CM
Número de vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		NNM	CM
DNI/T. Residencia/Pasaporte	Texto			R
NASS	Texto			CM
C/P de C. Autónoma	Texto			CM
Código SNS	Texto			R
C/P Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación	R
N.º Historia Clínica	Texto	Libre		CM
N.º Cama/N.º Consulta	Texto	Libre		R
DATOS DEL SOLICITANTE				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud.		CM
		SALUD. Servicio Aragonés de Salud		
		SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud		
		SCS. Servicio Cántabro de Salud.		
		SESCAM. Servicio de Salud de Castilla-La Mancha.		
		SACyL. Gerencia Regional de Salud de Castilla y León.		
		CatSS-GC. Departament de Salut de la Generalitat de Catalunya		
		SES. Servicio Extremeño de Salud.		
		SERGAS. Servizo Galego de Saúde.		
		INGESA. Instituto Nacional de Gestión Sanitaria.		
		IB-SALUT. Servicio de Salud de Illes Baleares.		
		RIOJASALUD. Servicio Riojano de Salud.		
		Servicio Madrileño de Salud.		
		Servicio Murciano de Salud.		
		SNS-O. Servicio Navarro de Salud-OSASUNBIDEA.		
		Agència Valenciana de Salut.		

Variable	Formato	Valores	Aclaraciones	Cl/I/F
		OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del proveedor de servicios	Texto + Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible + texto libre		CM
Dirección del Centro			Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	
Tipo de Vía	Texto			CM
Nombre de vía	Texto			CM
Número de vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la BD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		NNM	CM
DNI/T. Residencia/Pasaporte	Texto			R
NASS	Texto			CM
C/P de C. Autónoma	Texto			CM
Código SNS	Texto			R
C/P Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación	R
N.º Historia Clínica	Texto	Libre		CM
N.º Cama/N.º Consulta	Texto	Libre		R
DATOS DEL SOLICITANTE				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud.		CM
		SALUD. Servicio Aragonés de Salud		
		SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud		
		SCS. Servicio Cántabro de Salud.		
		SESCAM. Servicio de Salud de Castilla-La Mancha.		
		SACyL. Gerencia Regional de Salud de Castilla y León.		
		CatSS-GC. Departament de Salut de la Generalitat de Catalunya		
		SES. Servicio Extremeño de Salud.		
		SERGAS. Servizo Galego de Saúde.		
		INGESA. Instituto Nacional de Gestión Sanitaria.		
		IB-SALUT. Servicio de Salud de Illes Baleares.		
		RIOJASALUD. Servicio Riojano de Salud.		
		Servicio Madrileño de Salud.		
		Servicio Murciano de Salud.		
		SNS-O. Servicio Navarro de Salud-OSASUNBIDEA.		
		Agència Valenciana de Salut.		

Variable	Formato	Valores	Aclaraciones	Cl/I/F
		OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del proveedor de servicios	Texto + Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible + texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Servicio	Texto	Según normativa en vigor en cada momento	Actualmente clasificación de Servicios del CMBD/SIPCO	CM
Unidad	Texto	Libre		CM
Nombre del solicitante	Texto	Libre (nombre + 2 apellidos)		CM
Categoría profesional	Texto	Médico: Residente		CM
		Facultativo Especialista de Área		
		Jefe de Sección		
		Jefe de Servicio		
		Médico de Familia		
		Pediatra de AP		
		Texto libre		
DATOS DEL PROCESO ASISTENCIAL				
DATOS DE LA MUESTRA				
Fecha de toma de muestra	dd/mm/aaaa	Libre		CM
Número de muestra	Texto	Libre		CM
Tipo de muestra	Texto + Código	Libre		CM
		Bioquímica: LOINC		R
		Hematología: LOINC		
		Inmunología: LOINC		
		Genéticos: LOINC		
		Microbiología: Vocabulario local a partir de LOINC		
		A. Patológica Sn:mad-CT		
Grupo de determinación	Texto	Bioquímica general	*Bioquímica General*	CM
		Sistemático orina	*Metabólica (ej: glucosa, urea, creatinina, etc.)*	
		Hormonas	*Enzimas (AST, ALT, LDH, etc.)*	
		Marcadores tumorales	*Iones (Na, K, Cl, Ca, P, Mg, etc.)*	
		Niveles de fármacos y tóxicos	*Otras proteínas (Marcadores cardíacos, etc.)*	
		Gasometría Hematología	*Líquido Biológicos*	
		Hemostasia (Coagulación)	*Espermiogramas y estudios semen*	
		Hemoterapia	*Estudios en heces*	
		Hematología-Coagulación: Pruebas especiales	*Elementos traza (Cu, Se, etc.)*	
		Inmunología - Alergia	*Proteínas (Transferrina, Ceruloplasmina, Complemento, etc.)*	
		Microbiología Genética	*Electroforesis de proteínas*	
		Anatomía Patológica - Biopsias	*Inmunofijación/Inmunosubstracción*	
		Anatomía Patológica. Citologías	*Inmunoglobinas y Cadenas ligeras*	
			Sistemático orina:	
			Urianálisis	
			Sedimento	

Variable	Formato	Valores	Aclaraciones	DMR[2]
			Hormonas:	
			Hormonas	
			Vitaminas	
			Otros inmunoensayos relacionados (ej PAPPA)	
			Marcadores tumorales:	
			Marcadores tumorales séricos	
			Patología Molecular enfermedades neoplásicas hematológicas	

BOLETÍN OFICIAL DEL ESTADO
LEGISLACIÓN CONSOLIDADA

Variable	Formato	Valores	Aclaraciones	DMR[2]
			Patología Molecular enfermedades neoplásicas, tumores sólidos Niveles de fármacos y tóxicos: Monitorización de Fármacos Detección Drogas de abuso Detección de otros tóxicos (metales pesados, tóxicos laborales, etc.) Farmacogenómica Genometría Hematología: Hematimetría manual y automatizada (incluye el Hemograma, el diferencial leucocitario automatizado y manual, la morfología eritrocitaria, la VSG, la viscosidad plasmática, etc.) Hemostasia (coagulación): Pruebas de Hemostasia básicas (Tiempo de Protrombina, Tiempo de Tromboplastina Parcial Activada y Fibrinógeno) Hemoterapia: Estudios de Inmunohematología (detección de Anticuerpos irregulares) Pruebas de compatibilidad transfusional Hematología-Coagulación. Pruebas especiales: Citoquímica, Citometría, Citogenética y Biología Molecular de sangre periférica y médula ósea (incluye todos los marcadores diagnósticos) Aspirado medular y Biopsia de Médula Ósea (incluye todos los estudios de médula ósea) Estudios de Eritropatología Pruebas para estudio de Diátesis Hemorrágicas Pruebas para estudio de Trombosis Biología Molecular de alteraciones congénitas o adquiridas de la Hemostasia Inmunología-Alergia: Autoinmunidad Inmunoquímica Histocompatibilidad Inmunobiología Microbiología: Bacteriología Virología Parasitología	

Variable	Formato	Valores	Aclaraciones	CMI/R[6]
			Micología Serología infecciosa Biología molecular infecciosa Genética Citogenética Patología/Genética molecular Anatomía Patológica-Biopsias Biopsias y piezas quirúrgicas Inmunohistoquímica Anatomía Patológica molecular Microscopía electrónica Citometría de flujo	
			Anatomía Patológica-Citologías Citologías y PAAF Inmunocitoquímica Anatomía Patológica molecular Microscopía electrónica Colorimetría de flujo	
Modelo TIPO A			Este modelo puede recoger todos aquellos resultados de pruebas diagnósticas que se expresan con una denominación de determinación, un resultado (generalmente expresado en cifras), las unidades de medida utilizadas y un rango de valores de referencia que se toman como estándar de normalidad.	
Determinación	Texto	Libre		CM
Resultado	Texto	Libre		CM
Unidades	Texto	Libre		CM
Rango	Texto	Libre		CM
Comentarios	Texto	Libre		R
Modelo TIPO B			Este modelo puede recoger todos aquellos resultados de pruebas diagnósticas que requieren una descripción y una conclusión en texto libre. Ej. Estudio de médula ósea.	
Determinación	Texto	Libre		CM
Técnica	Texto			CM
Descripción	Texto	Libre		CM
Conclusión	Texto +	Libre		CM
	Código	SNOMED		R

[6] Se puede clasificar cada campo según se considere que su presencia en esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debo formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R).

[4] CNH: Catálogo Nacional de Hospitales.

[7] RECESS: Registro General de Establecimientos, Centros y Servicios Sanitarios del MSPS.

ANEXO VI

CONJUNTO DE DATOS DEL INFORME DE RESULTADOS DE PRUEBAS DE IMAGEN

Variable	Formato	Valores	Aclaraciones	CMI/R[6]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe de resultados de pruebas de imagen		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	CM
Nombre Responsable 1	Texto	Libre (nombre+2 apellidos)		CM
Categoría profesional 1	Texto	Médico Residente Facultativo Especialista de Área Jefe de Sección Jefe de Servicio	Es parte del primer pie de firma del informe	CM
Nombre Responsable 2	Texto	Libre (nombre+2 apellidos)		CM
Categoría profesional 2	Texto	Facultativo Especialista de Área Jefe de Sección Jefe de Servicio	Es parte del segundo pie de firma, que suele supervisar al primer firmante	
Servicio	Texto	Radiodiagnóstico Medicina Nuclear		CM
Unidad	Texto	Libre		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud. SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud. ICS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL. Gerencia Regional de Salud de Castilla y León. CatSalut. Departament de Salut de la Generalitat de Catalunya. SES. Servicio Extremeño de Salud. SERGAS. Servio Gallego de Salude. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud. SNS-O. Servicio Navarro de SaludOSASUNBIDEA. Agència Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM
Denominación del proveedor de servicios	Texto + Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH y posteriormente RECESS cuando esté disponible+texto libre		CM
Dirección del Centro				
Tipo de vía	Texto			CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto	CNH y posteriormente RECESS cuando esté disponible+texto libre		CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				

Variable	Formato	Valores	Aclaraciones	CM/R[4]
Nombre	Texto	Dato que figure en la BD de la TSI de la CA.		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T. Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de C.Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación	R
N.º Historia Clínica	Texto	Libre		CM
N.º Cama / N.º Consulta	Texto	Libre		R
DATOS DEL SOLICITANTE				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha.		CM
		SACyL. Gerencia Regional de Salud de Castilla y León. CatSalut. Servicio Catalán de la Salud. SES. Servicio Extremeño de Salud. SERGAS. Servicio Gallego de Salud. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud/OSASUNBIDEA. Agencia Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		
Denominación del proveedor de servicios	Texto + Logo	Libre		R
Denominación del Centro	Texto + Logo	CNH[5] y posteriormente RECESS[6] cuando esté disponible-texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el inventario en vigor por ser de reciente apertura	CM
Servicio	Texto	Según normativa en vigor en cada momento	Actualmente clasificación de Servicios del CNISS/SIFCO	CM
Unidad	Texto	Libre		CM
Nombre del solicitante	Texto	Libre (nombre+2 apellidos)		CM
Categoría profesional	Texto	Médico Residente Facultativo Especialista de Área Jefe de Sección Jefe de Servicio Médico de Familia Facultativo Pediatra de AP Texto Libre		CM
DATOS DEL PROCESO ASISTENCIAL				
Información Clínica	Texto	Libre	Reflejará el mismo contenido que el volante de petición de la exploración. Es el lugar para detallar los datos clínicos que justifican la realización de la prueba y establecen las sospechas diagnósticas	CM
Exploración	Texto + Código (cadena numérica+ cadena de texto)	Libre Catálogo SETAM en vigor Catálogo SEMN en vigor		CM R
Fecha de Exploración	dd/mm/aaaa	Libre		CM
Descripción de la exploración	Texto	Libre	Es una descripción detallada de la exploración realizada, en la que podrán concretarse además: Prioridad (normal, urgente) Medios de contraste (tipo, dosis y velocidad de inyección Reacciones adversas Otras incidencias (falta de colaboración, ansiedad, claustrofobia…) y abordaje de los mismos. Limitaciones técnicas Exploración con la que se compara y fecha de la misma	R

Variable	Formato	Valores	Aclaraciones	CM/R[4]
Hallazgos	Texto	Libre	Es una descripción detallada de los hallazgos, en la que podrán concretarse además: Hallazgos negativos	CM
			Comparación con estudios previos Limitaciones diagnósticas	
Diagnóstico	Texto + Código	Libre Cadena de texto (Nombre del catálogo utilizado) + Código asignado		CM R
Recomendaciones	Texto	Libre	Es el lugar para recoger: Cuidados o tratamientos que se deben seguir después de la realización de la exploración diagnóstica o intervencionista. Indicación de otras exploraciones que se deban realizar para completar el estudio del paciente o el plazo en el que se debe realizar un control de la exploración	CM

[4] Se puede clasificar cada campo según se considere que su presencia en esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debo formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R).

[5] CNH: Catálogo Nacional de Hospitales.

[6] RECESS: Registro General de Establecimientos, Centros y Servicios Sanitarios del MSPS.

ANEXO VII

CONJUNTO DE DATOS DEL INFORME DE CUIDADOS DE ENFERMERÍA

Variable	Formato	Valores	Aclaraciones	CM/R[11]
DATOS DEL DOCUMENTO				
Tipo de documento	Texto	Informe de Cuidados de Enfermería		CM
Fecha de firma	dd/mm/aaaa	Libre	Es común a ambos pies de firma del informe	CM
Fecha Valoración de Enfermería	dd/mm/aaaa	Libre		CM
Fecha Alta de Enfermería/Fecha de Derivación Enfermera	dd/mm/aaaa	Libre		CM
Enfermera Responsable 1	Texto	Libre (nombre+2 apellidos)	Es parte del primer pie de firma del informe	CM
Categoría profesional Enfermera Responsable 1	Texto	Enfermera Enfermera Especialista Enfermera Residente (EIR)		CM
Enfermera Responsable 2	Texto	Libre (nombre+2 apellidos)	Es parte del segundo pie de firma, que suele supervisar el primer firmante	CM
Categoría profesional Enfermera Responsable 2	Texto	Enfermera Enfermera Especialista		CM
Dispositivo Asistencial	Texto	Centro de Salud Hospital Urgencias Hospitalarias Urgencias Extrahospitalarias Centro Sociosanitario Otros		CM
DATOS DE LA INSTITUCIÓN EMISORA				
Denominación del Servicio de Salud	Texto + Logo	SAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL. Gerencia Regional de Salud de Castilla y León. CatSalut. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS. Servicio Gallego de Salud. INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agencia Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM
Denominación del proveedor de servicios	Texto + Logo	Libre		R

Variable	Formato	Valores	Aclaraciones	CM/R [1]
Denominación del Centro	Texto + Logo	CNH [2] para Centros de Atención Especializada, Inventario para Centros de Primaria y posteriormente RECESS [3] cuando esté disponible + texto libre		CM
Dirección del Centro				
Tipo de vía	Texto	CNH y posteriormente RECESS cuando esté disponible +texto libre	Existirá un campo adicional de texto libre para aquellos centros no recogidos en el Inventario en vigor por ser de reciente apertura	CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
País	Texto			CM
Teléfono	Texto			CM
Dirección Web/Correo electrónico	Texto	Libre	Se incluirá la dirección Web sólo si contiene información de interés para el usuario	R
DATOS DEL PACIENTE				
Nombre	Texto	Dato que figure en la SD de la TSI de la CA		CM
Primer Apellido	Texto			CM
Segundo Apellido	Texto			CM
Fecha nacimiento	dd/mm/aaaa			CM
Sexo	Texto		H/M	CM
DNI/T. Residencia/Pasaporte	Texto			R
NASS	Texto			CM
CIP de C Autónoma	Texto			CM
Código SNS	Texto			R
CIP Europeo	Texto		Se reserva este espacio en previsión de que, en el futuro, exista un código europeo/internacional de identificación.	R
N.º Historia Clínica	Texto	Libre		CM
Domicilio				
Tipo de vía	Texto	Dato que figure en la SD de la TSI de la CA		CM
Nombre de la vía	Texto			CM
Número de la vía	Texto			CM
Piso	Texto			CM
Letra	Texto			CM
Código Postal	Texto			CM
Municipio	Texto			CM
Provincia	Texto			CM
Teléfono	Texto	Dato que figure en la SD de la TSI de la CA+texto libre	Existirá texto libre para añadir un segundo número de teléfono	R
Persona de Referencia	Texto	Libre (nombre + 2 apellidos)	Se trata de la persona que representa los intereses del paciente.	CM
Teléfono de Referencia	Texto	Libre		CM
DATOS DEL PROCESO ASISTENCIAL				
Causas que generan la actuación enfermera	Texto	Libre		CM
Motivo de Alta/Derivación Enfermera	Texto	Ingreso Traslado a domicilio Traslado de Servicio Traslado a centro hospitalario Traslado a un centro sociosanitario Alta voluntaria Fallecimiento Otros		CM
Antecedentes y entorno	Texto	Libre	Destacar solamente la información relevante	CM
Enfermedades Previas Intervenciones quirúrgicas Tratamientos farmacológicos Alergias Actuaciones preventivas (1) Factores personales, familiares, sociales, culturales y laborales destacables (2).	Texto	Libre	(1) Vacunaciones y su estado (2) El conjunto de factores resaltados se refiere a aquellos elementos (personales, familiares, sociales o profesionales) que, formando parte de su entorno, pueden influir o condicionar la evolución de su estado de salud. Tienen cabida también aquellos acontecimientos puntuales (pérdida de familiar, evento laboral...) que puedan influir en su respuesta ante diferentes situaciones de salud.	R

Variable	Formato	Valores	Aclaraciones	CM/R [1]
Diagnósticos Enfermeros resultados	Texto + código	Libre/ NANDA + Código NANDA	Se trata de destacar aquellos diagnósticos, ya resueltos, que puedan resultar de interés para prever posteriores apariciones	CM R
Protocolos asistenciales en los que está incluido	Texto	Libre	Tienen cabida todos los procesos asistenciales y programas de salud en los que se encuentre incluido, tanto programas preventivos como de seguimiento, rehabilitación o educación sanitaria entre otros. Así como la relación de problemas interdependientes y/o de colaboración si fuera el caso.	CM
Valoración activa	Texto	Libre		CM
Modelo de referencia utilizado Resultados destacables	Texto	Libre	Deberá reflejarse la información relativa a la valoración enfermera más reciente. Se recomienda especificar otras escalas o tests aplicados y ajenos al modelo utilizado en la valoración general.	CM CM
Diagnósticos Enfermeros activos	Texto + código	Libre/ NANDA + Código NANDA	Aquellos diagnósticos presentes en el momento de la elaboración del informe, tanto reales como potenciales	CM R
Resultados de Enfermería	Texto + código	Libre/ NOC + Código NOC	Aquellos resultados seleccionados para identificar la evolución del paciente, como resultado de las intervenciones planificadas	CM R
Intervenciones de Enfermería	Texto + código	Libre/ NIC + Código NIC	Las intervenciones que se están llevando a cabo en el momento de elaboración del informe	CM R
Cuidador principal	Texto	Libre (nombre + 2 apellidos) + Vinculación con el usuario	Deberá indicarse tanto el nombre como la relación que tiene con él (familiar, cuidador externo...)	CM R
Información complementaria/ Observaciones	Texto	Libre	Puede incluirse información relativa a la presencia de catéteres, prótesis, dietas especiales, así como destacar algún aspecto de especial relevancia relativo a la aplicación de las intervenciones activas.	R

[1] Se puede clasificar cada campo según se considere que su presencia es esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debo formar parte del conjunto mínimo del SNS (CM) o por el contrario es aconsejable su presencia pero no imprescindible como parte del conjunto mínimo de datos (R).

[2] CNH: Catálogo Nacional de Hospitales.

[3] RECESS: Registro General de Establecimientos, Centros y Servicios Sanitarios del MSPS.

ANEXO VIII

CONJUNTO DE DATOS DE LA HISTORIA CLÍNICA RESUMIDA

Variable	Formato	Valores	Aclaraciones	CM/R [1]	Volcado de Datos [2]	Acceso [3]
DATOS DEL DOCUMENTO						
Tipo de documento	Texto	Historia Clínica Resumida		CM	A	P/C
Fecha de creación	dd/mm/aaaa	Libre		CM	A	P/C
Fecha de última actualización	dd/mm/aaaa	Libre	La fecha en la que fue modificado alguno de los componentes del registro por última vez	CM	A	P/C
DATOS DE LA INSTITUCIÓN EMISORA						

Variable	Formato	Valores	Aclaraciones	CM/R[13]	Volcado de Datos[14]	Acceso[15]
Denominación del Servicio de Salud	Texto + logo	DAS. Servicio Andaluz de Salud. SALUD. Servicio Aragonés de Salud SESPA. Servicio de Salud del Principado de Asturias. Servicio Canario de Salud SCS. Servicio Cántabro de Salud. SESCAM. Servicio de Salud de Castilla-La Mancha. SACyL. Gerencia Regional de Salud de Castilla y León. SatS-GC. Departament de Salut de la Generalitat de Catalunya SES. Servicio Extremeño de Salud. SERGAS.Servizo Galego de Saúde INGESA. Instituto Nacional de Gestión Sanitaria. IB-SALUT. Servicio de Salud de Illes Balears. RIOJASALUD. Servicio Riojano de Salud. Servicio Madrileño de Salud. Servicio Murciano de Salud. SNS-O. Servicio Navarro de Salud-OSASUNBIDEA. Agéncia Valenciana de Salut OSAKIDETZA-Servicio Vasco de Salud.		CM	A	P/C
Denominación del proveedor de servicios	Texto+logo	Libre		R		
DATOS DEL USUARIO/PACIENTE						
Nombre	Texto	Dato que figure en BD de TSI de la CA		CM	A	P/C
Primer Apellido	Texto			CM	A	P/C
Segundo Apellido	Texto			CM	A	P/C
Fecha de nacimiento	dd/mm/aaaa			CM	A	P/C
Sexo	Texto		H/M	CM	A	P/C
DNI/T. Residencia/Pasaporte	Texto			R	A	P/C
NASS	Texto			CM	A	P/C
CIP de C. Autónoma	Texto			CM	A	P/C
Código SNS	Texto			R	A	P/C
CIP Europeo			Se reserva este espacio en previsión de que en el futuro exista un código europeo/internacional de identificación.	R	A	P/C
N.º Historia Clínica	Texto	Libre		CM	A	P/C
Tipo de vía	Texto	Dato que figure en la BD de TSI de la CA		CM	A	P/C
Nombre de la vía	Texto			CM	A	P/C
Número de la vía	Texto			CM	A	P/C
Piso	Texto			CM	A	P/C
Letra	Texto			CM	A	P/C
Código Postal	Texto			CM	A	P/C
Municipio	Texto			CM	A	P/C
Provincia	Texto			CM	A	P/C
Teléfono	Texto			R	A	P/C
Persona de referencia	Texto	Libre (nombre + 2 apellidos)	Se trata de la persona que representa los intereses del paciente.	R	A/M	P/C
Teléfono de referencia	Texto	Libre		R	A/M	P/C
Cuidador Principal	Texto	Libre (nombre + 2 apellidos)		R	A/M	P/C
DATOS DE SALUD						
Existe información reservada por decisión del paciente	Solor s/n	SI NO	Este campo informa al profesional de que existe según dato clínico que no figura en la HC por decisión del propio paciente.	CM	A	P/C
Existe documento de instrucciones previas	Solor s/n	SI NO	Informa al profesional de que existe este documento que está disponible en el Registro de Últimas Voluntades.	CM	A/M	P/C
Está incluido en protocolo de investigación clínica	Solor s/n	SI NO	Informa de la inclusión en un protocolo de investigación en la fecha de última actualización.	R	M	P/C
Alergias	Texto	Libre		CM	A	P/C
Vacunaciones	Texto	Libre		CM	A	P/C

Variable	Formato	Valores	Aclaraciones	CM/R[13]	Volcado de Datos[14]	Acceso[15]
Problemas Resueltos, Cerrados o Inactivos	Texto	Fecha + Texto Libre	Se especificará la fecha de cierre y el motivo	R	A	P/C
Problemas y Episodios Activos	Texto + Código	Fecha + Texto libre Sistema de Codificación CIE 9 MC/CIE 10/CIAP 2 Definida/SNOMED-CT	Los que figuren en la historia a la fecha de última actualización. Los sistemas de codificación serán sustituidos por versiones posteriores si así se acordara en el Consejo Interterritorial del SNS	CM R	A	P/C
Tratamiento	Texto	Libre		CM		P/C
Recomendaciones	Texto	Libre	Se trata de recomendaciones terapéuticas que no incluyen fármacos (psicoterapia, dieta, limitaciones de esfuerzo físico, etc.)	CM	A	P/C
Fármaco	Texto + código	Libre (Especialidad + principio activo + dosis/unidad> nº unidades/dosis> intervalo de dosis> vía administración> duración); nomenclator oficial INGPS (código nacional)/Snomed-CT	Prescripciones activas a la fecha de actualización. En la medida en que la implantación de las aplicaciones informáticas de HCE, que incluyan módulos de prescripción lo permitan, el texto libre, será reemplazado progresivamente por el vocabulario del catálogo de medicamentos autorizados (Nomenclator Oficial/Snomed-CT)	CM	A	P/C
Diagnósticos Enfermeros activos	Texto + Código	Literal NANDA +Código NANDA	Los que figuren en la historia a la fecha de última actualización	CM R	A	P/C
Resultados de Enfermería	Texto + Código	Literal NOC +Código NOC	Aquellos resultados seleccionados para identificar la evolución del paciente, como resultado de las intervenciones planificadas. Los que figuren en la historia a la fecha de última actualización	CM R	A	P/C
Intervenciones de Enfermería	Texto + código	Literal NIC +Código NIC	Los que figuren en la historia a la fecha de última actualización	CM R	A	P/C
ALERTAS	Texto	Libre	Su contenido deben ser advertencias clave de carácter objetivo que por su especial trascendencia deban ser resaltadas para ser tenidas en cuenta por cualquier profesional que deba prestar atención (E: Angioedema desencadenado por IECAS, Dispositivo IV con reservorio)	CM	M	P/C
Observaciones Subjetivas del Profesional	Texto	Libre	La única justificación de este campo es recoger valoraciones del profesional, siempre que sean de auténtico interés para el manejo de los problemas de salud por otro profesional. Sólo deberán ser reseñadas aquellas observaciones que sean encuadrables en algunos de los siguientes apartados: · VALORACIONES SOBRE HIPÓTESIS DIAGNÓSTICAS NO DEMOSTRADAS · SOSPECHA ACERCA DE INCUMPLIMIENTOS TERAPÉUTICOS · SOSPECHA DE TRATAMIENTOS NO DECLARADOS	R	M	P
			SOSPECHA DE HÁBITOS NO RECONOCIDOS			
			SOSPECHA DE HABER SIDO VÍCTIMA DE MALOS TRATOS			
			COMPORTAMIENTOS INSÓLITOS			

[13] Se puede clasificar cada campo según se considere que su presencia en esencial (aunque la cumplimentación del valor no sea obligatoria) y por ello debe formar parte del conjunto mínimo del SNS (CM), o por el contrario es aconsejable su presencia, pero no imprescindible como parte del conjunto mínimo de datos (R).

[14] Los datos de los campos de la Historia Clínica Resumida deben alimentarse de forma automática A, a partir de la historia de salud digital, excepto un número muy reducido de ellos que tendrá que alimentar manualmente M el profesional, en aquellos casos en que éste lo considere conveniente.

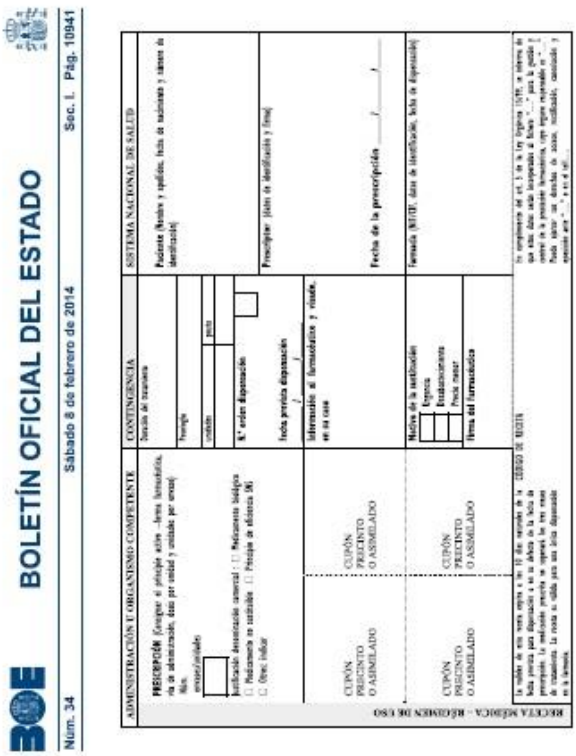
[15] El campo puede estar accesible, según la naturaleza de su contenido (anotaciones subjetivas o datos objetivos), a los profesionales P o al ciudadano C.

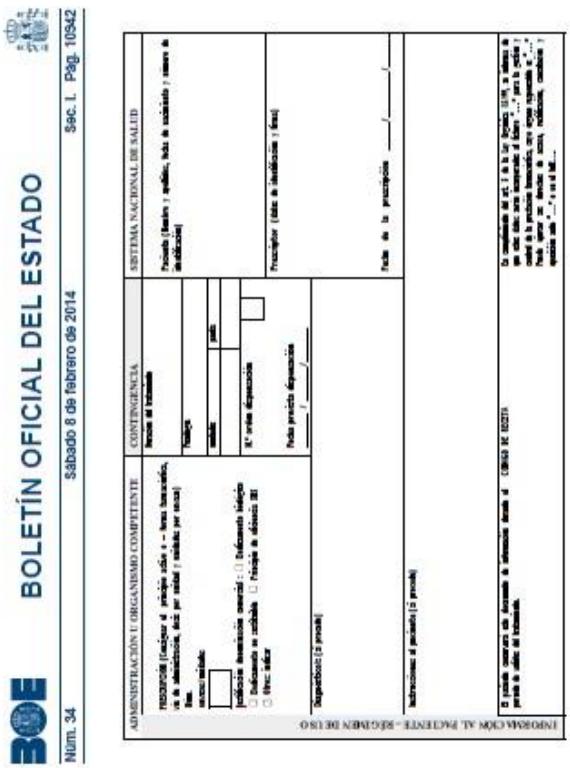
ANEXO IX

LISTADO ALFABÉTICO DE ABREVIATURAS EMPLEADAS

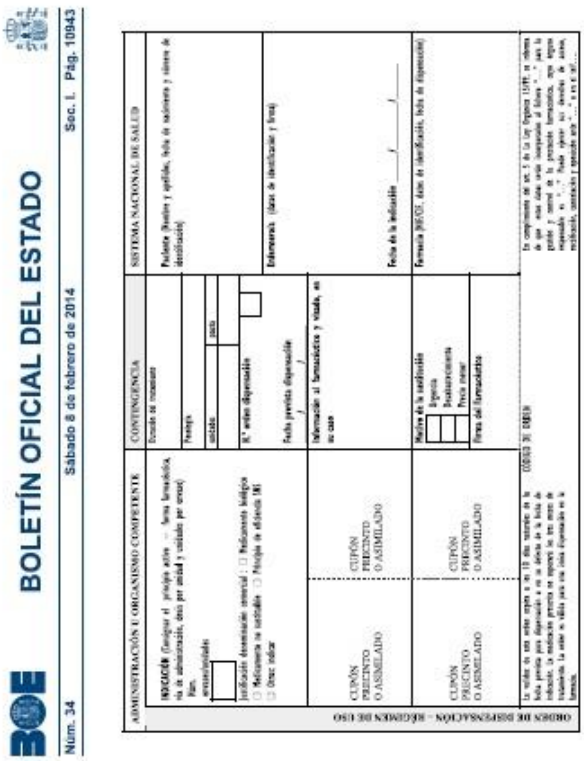
Abreviatura empleada	Significado
BD TSI	Base de datos de tarjeta sanitaria individual.

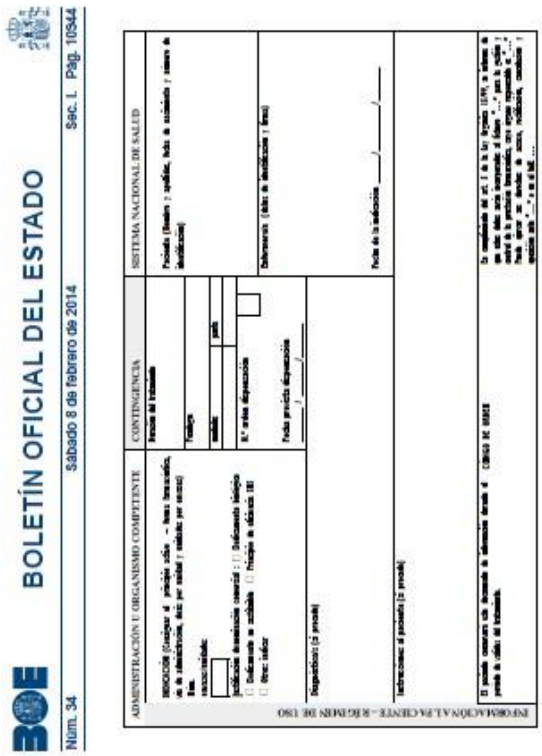
Anexo [BB] Receta médica. Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.





Anexo [CC] Orden de dispensación. Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.





Anexo [DD] Receta electrónica. Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación

BOLETÍN OFICIAL DEL ESTADO
Núm. 34 Sábado 8 de febrero de 2014 Sec. I. Pág. 10545

Sistema de Receta Electrónica del Sistema Nacional de Salud

HOJA DE MEDICACIÓN ACTIVA E INFORMACIÓN AL PACIENTE

ADMINISTRACIÓN U ORGANISMO COMPETENTE	Nombre y apellidos del prescriptor/ enfermero Dirección Población	PACIENTE (Nombre y apellidos) y número de identificación	Fecha Nacimiento
		Fecha de emisión ____/____/____	
Régimen de uso	N.º Colegiado o N.º de Identificación Especialidad	Firma del prescriptor/enfermero	

Código o Número de prescripción	Prescripción/Indicación (Consignar el medicamento – forma farmacéutica, vía de administración, dosis por unidad y número de unidades por envase)	Posología		Duración del tratamiento
		Unidades	Pauta	

Diagnóstico/s (si procede)

Instrucciones para el paciente:

El paciente autoriza el acceso por el farmacéutico a los tratamientos incluidos en esta relación.
El paciente conservará esta documentación informativa durante el periodo de validez del tratamiento.
En cumplimiento del art. 5 de la Ley Orgánica 15/99, le informamos de que estos datos serán incorporados al fichero "..." para la gestión y control de la prestación farmacéutica, cuyo órgano responsable es "..." Puede ejercer sus derechos de acceso, rectificación, cancelación y oposición ante "..." o en el BdE. ...

cve: BOE-A-2014-1331

Anexo [EE] Receta de estupefacientes. Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación

Receta oficial de estupefacientes para uso humano

RECETA OFICIAL DE ESTUPEFACIENTES	Duración del tratamiento	PACIENTE (Nombre y apellidos, año de nacimiento, DNI/NIE o número de identificación)
PRESCRIPCIÓN (Consignar el medicamento – forma farmacéutica, vía de administración, dosis por unidad y unidades por envase) **Número envases/unidades**	Posología unidades / pauta	**PRESCRIPTOR** (datos de identificación, teléfono y firma) Fecha de la prescripción / /
ESPACIO DESTINADO PARA CONTROL Y PROCESAMIENTO	ADMINISTRACIÓN COMPETENTE SELLO DE VALIDACIÓN ENTIDAD DISTRIBUIDORA	**FARMACIA** (NIF/CIF, datos de identificación, fecha de la dispensación y firma)
La validez de esta receta expira a los 10 días naturales de la fecha de prescripción. La medicación prescrita no superará los tres meses de tratamiento.	CÓDIGO DE RECETA CÓDIGO DE BARRAS	

En cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa de que estos datos serán incorporados al fichero..., para la gestión y control de los medicamentos estupefacientes. Puede ejercer sus derechos de acceso, rectificación, cancelación y oposición ante "..." o en el teléfono "...".

Hoja de información al paciente

HOJA DE INFORMACIÓN AL PACIENTE RECETA OFICIAL DE ESTUPEFACIENTES	Duración del tratamiento	PACIENTE (Nombre y apellidos, año de nacimiento, DNI/NIE o número de identificación)
PRESCRIPCIÓN (Consignar el medicamento – forma farmacéutica, vía de administración, dosis por unidad y unidades por envase) **Núm. Envases/unidades**	Posología	**PRESCRIPTOR** (datos de identificación, teléfono y firma) Fecha de la prescripción / /
Diagnóstico (si procede)	Unidades / Pauta	
Instrucciones para el paciente (si procede)		
El paciente conservará este documento de información durante el período de validez del tratamiento.	CÓDIGO DE RECETA CÓDIGO DE BARRAS	

En cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa de que estos datos serán incorporados al fichero..., para la gestión y control de los medicamentos estupefacientes. Puede ejercer sus derechos de acceso, rectificación, cancelación y oposición ante "..." o en el teléfono "...".

Anexo [FF] tarjeta sanitaria. Real Decreto 702/2013, de 20 de septiembre, por el que se modifica el Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

BOLETÍN OFICIAL DEL ESTADO
Núm. 238 Viernes 4 de octubre de 2013 Sec. I. Pág. 81575

Dos. Se modifica el artículo 8 que queda redactado de la siguiente manera:

«Artículo 8. *Colectivos asegurados a través de regímenes especiales.*

A cada titular y beneficiario asegurado a través de regímenes especiales le será expedida una tarjeta sanitaria, con las adecuaciones derivadas de las características de estos regímenes de aseguramiento, con soporte informático, con las características básicas que se definen en este real decreto incluida la asignación de un código de identificación personal del Sistema Nacional de Salud. Los datos de dicha tarjeta sanitaria se incorporarán al sistema de intercambio de información que proporciona la base de datos de población protegida del Sistema Nacional de Salud.»

Tres. Se incorpora un anexo con la siguiente redacción:

ANEXO

1. Anverso

Modelo sin fotografía

Modelo con fotografía

Descripción:

Ángulo superior izquierdo: Imagen institucional de la administración sanitaria emisora o fotografía del titular de la tarjeta sanitaria.

Franja superior o universal:

1.ª línea (a la derecha): SISTEMA NACIONAL DE SALUD DE ESPAÑA (Arial Narrow, 9 pt, negrita). Rótulo.
2.ª línea (a la derecha): Tarjeta Sanitaria (TNRoman, 10 pt, negrita). Rótulo.

cve: BOE-A-2013-10030

BOLETÍN OFICIAL DEL ESTADO
Núm. 238 Viernes 4 de octubre de 2013 Sec. I. Pág. 81576

Franja media:

Entre la segunda línea de la franja superior y la primera línea de la franja inferior se incluirá la imagen institucional de la administración sanitaria emisora de la tarjeta en el caso que en el ángulo superior izquierdo se sitúe la fotografía del titular.

Franja inferior

1.ª línea: BGKX004499816015 (TNRoman, 11 pt, negrita).
(Código de identificación personal asignado por la administración sanitaria que emite la tarjeta)
2.ª línea: Adicionales

DNI/NIE	Núm. SS	Fecha caducidad	Teléfono urgencias
98979695R	58/68752834/56	02/16	999 999 999

(TNRoman, 9 pt, normal)

– Formato DNI: ocho dígitos y letra de control.
– Formato NIE: letra inicial, siete dígitos y letra final de control.
– Formato Número Seguridad Social: doce dígitos, dos de provincia, ocho de orden y dos de control.
– Formato Fecha de caducidad: mm/aa.
– Formato Teléfono: máximo nueve dígitos.

3.ª línea: NOMBRE APELLIDO PRIMERO APELLIDO SEGUNDO

(TNRoman, 9 pt, negrita).
(Hasta 40 caracteres, si tiene más el punto de truncado sería el último carácter. De ser necesarios más caracteres se minorará el tipo de letra respetando en todo caso la inclusión de los datos en una única línea).
CIPSNS CITE TSI

4.ª línea: BBBBBBBBQR648597 807240000122 Braille

(Ambos códigos NTRoman, 9 pt, negrita) (si procede).
CIPSNS: 16 caracteres alfanuméricos.
CITE (Código administración sanitaria emisora de la tarjeta): once dígitos (según norma UNE- EN 1387:1997) en el siguiente orden:

– 2 dígitos: área de actividad (80).
– 3 dígitos: código país norma ISO 3166.
– 5 dígitos: código de la entidad que emite la tarjeta.
– 1 dígito de control.

Ángulo inferior derecho: A instancia de parte, o de oficio en aquellas administraciones sanitarias que así lo prevean en su normativa, se grabarán en Braille los caracteres de las iniciales de Tarjeta Sanitaria Individual, siguiendo la norma UNE-EN 1332.1:2010, en su parte 5 de marzo de 2006.

2. Reverso:

Banda magnética con tres pistas:

Pista 1 alfanumérica:

– CIP-xx asignado por la administración sanitaria emisora de la tarjeta.
– CIP-SNS único asignado por el Sistema Nacional de Salud.

cve: BOE-A-2013-10536

BOLETÍN OFICIAL DEL ESTADO
Núm. 238 Viernes 4 de octubre de 2013 Sec. I. Pág. 81577

– Código de la administración sanitaria emisora (dos dígitos, el software de lectura convertirá este código al CITE que figura en el anverso de la tarjeta).
– Nombre y apellidos del titular.

Pista 2 numérica: libre.
Pista 3 regrabable.

3. Características específicas:

Tamaño de la tarjeta: ID1 siguiendo los estándares ISO 7810 de 1985.
Si la tarjeta incorpora chip su ubicación se atendrá a la norma UNE-EN 1387:1997.
Banda magnética, de alta coercitividad, de lectura-escritura, con tres pistas, norma ISO 7811 de 1985.

Disposición adicional única. *Sustitución de tarjetas sanitarias individuales.*

El proceso de sustitución de las actuales tarjetas se llevará a cabo de forma progresiva, con motivo de su renovación por cualquier causa o de nuevas emisiones, debiendo estar finalizado antes de cinco años contados a partir de la entrada en vigor de este real decreto, siempre que las disponibilidades presupuestarias de las diferentes administraciones públicas competentes lo permitan.

Disposición final única. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid, el 20 de septiembre de 2013.

JUAN CARLOS R.

La Ministra de Sanidad, Servicios Sociales e Igualdad,
ANA MATO ADROVER

cve: BOE-A-2013-10006

http://www.boe.es BOLETÍN OFICIAL DEL ESTADO D. L.: M-1/1958 - ISSN: 0212-033X

Anexo GG Circulación-movimiento de la historia clínica en el Hospital Universitario La Paz

consulta el paciente; pero al alta y previamente a su envío a Archivo todos los documentos deberán ser colocados por orden de numeración por el administrativo del servicio.

El Servicio de Documentación y Archivos velará para que todas las historias clínicas mantengan el ORDEN y podrá devolver al servicio de procedencia, para su reordenación, toda historia clínica que no mantenga dicho orden.

3. CIRCULACION-MOVIMIENTO DE LA HISTORIA CLINICA EN EL HOSPITAL

El control de la documentación clínica será responsabilidad del Servicio de Documentación Clínica, que controlará el movimiento y uso de dicha documentación.

El Archivo de Historias clínicas tiene como objetivo fundamental guardar y custodiar la documentación clínica que generen los pacientes. Una vez dado el paciente de alta, y realizado el correspondiente informe médico, la historia clínica se enviará al Archivo en un plazo menor de 24 horas si ha sido utilizada en consultas externas y de 48 horas las procedentes de hospitalización.

Todas las historias clínicas deberán guardarse en el Archivo y éste por tratamiento informático podrá conocer en todo momento los movimientos de las mismas.

3.1 CONSERVACIÓN Y DESTRUCCIÓN DE LA HISTORIA CLÍNICA

Según la ley 41/2002 básica reguladora de la autonomía del paciente…:

1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en su soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y

6

Anexo [HH] Procedimiento de inclusión de nuevo Documento en la historia clínica en el Hospital Universitario La Paz

Hospital Universitario La Paz
Hospital de Cantoblanco
Hospital Carlos III
SaludMadrid
Comunidad de Madrid

Procedimiento de Inclusión de Nuevo Documento en la Historia Clínica

REVISADO Y APROBADO POR: **COMISIÓN DE DOCUMENTACIÓN CLÍNICA**	Fecha: 26 de octubre de 2015
ELABORADO Y APROBADO POR: **COMISIÓN DE DOCUMENTACIÓN CLÍNICA** (Acta 1/2010)	Fecha: 13 de enero de 2010

ÍNDICE.

INTRODUCCIÓN:

Entre las funciones de la Comisión de Documentación Clínica del Hospital Universitario La Paz, se encuentran:

Definir los procesos y establecer los procedimientos para el uso de la documentación y registros clínico-administrativos y de la información desprendida de los mismos.

Evaluación de los documentos de registro de actividad clínica contribuyendo a su normalización y participando en el diseño de los mismos.

Dar apoyo técnico a profesionales, departamentos, servicios o comisiones que así lo requieran.

Transcurridos 5 años desde la publicación por parte de la comisión de documentación clínica del Procedimiento de Inclusión de Nuevo Documento en la Historia clínica, y en pleno proceso de instauración de la nueva historia clínica electrónica, se ha considerado adecuado revisar dicho procedimiento y proceder a su posterior publicación en la intranet del hospital.

Además se ha tratado de adecuar dicho procedimiento a la nueva situación que se va a crear con la historia clínica electrónica

Objeto:

Este documento tiene por objeto reflejar el procedimiento a seguir para la inclusión de nuevos documentos en la Historia Clínica, partiendo de la solicitud documentada hasta la aprobación por parte de la Dirección del Centro.

Alcance:

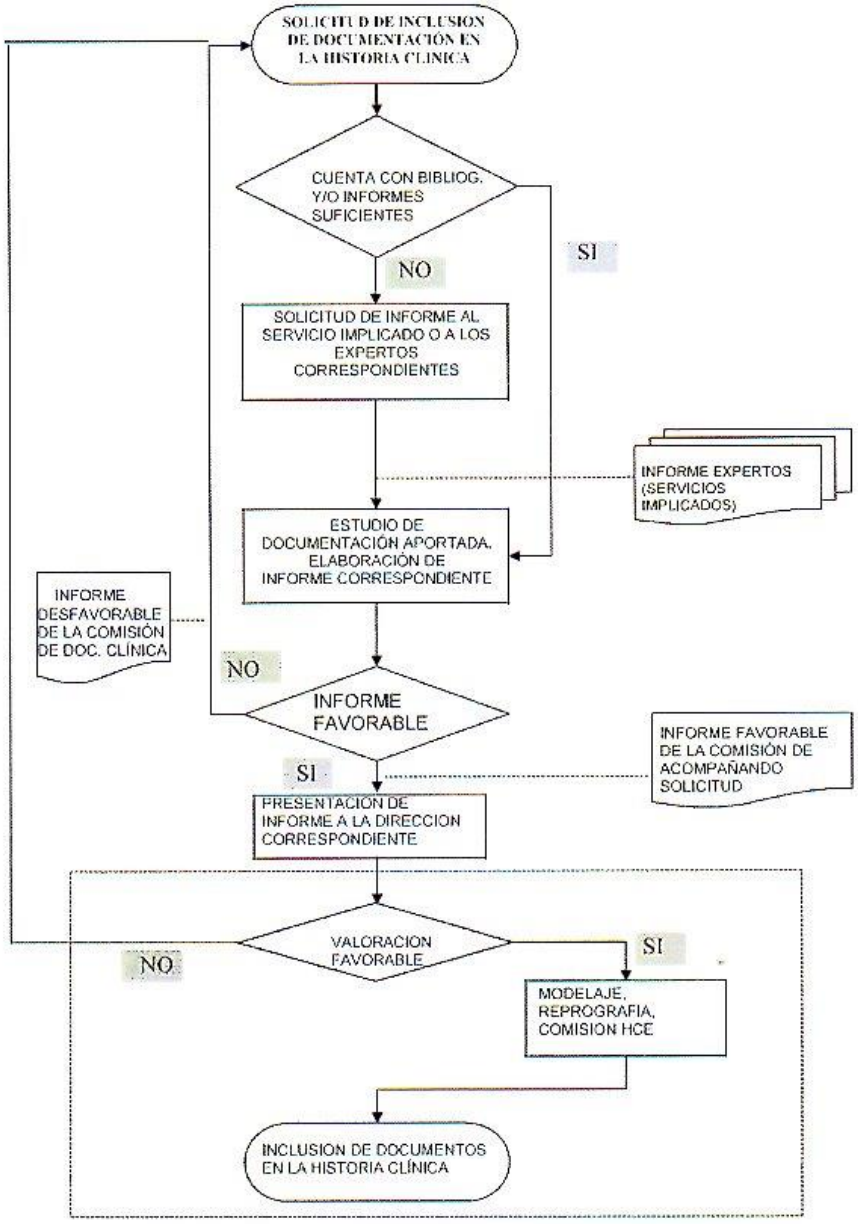
El procedimiento afecta a todos los Servicios, Departamentos y Unidades que propongan incluir un nuevo documento en la Historia Clínica del Hospital y que precisen contar con el informe y aprobación de esta Comisión. Queda entendido que, a partir de este momento, cualquier otro documento que se incluya en la Historia Clínica sin seguir este circuito, no cuenta con el apoyo de esta Comisión.

Documentos aplicables:

Guía de Documentación Clínica – H.U. La Paz, apartados 3.1 y 3.4.2

Hospital Universitario La Paz	COMISIÓN DE DOCUMENTACIÓN CLÍNICA	
		Cod:
	SOLICITUD INCLUSION DOC. CLÍNICA	REVISIÓN 01

Diagrama de flujo.



Página 4 de 6

Descripción de las actividades:

Para asegurar que el documento propuesto cuenta con el debido estudio y consenso, entendemos que toda solicitud de inclusión de documentación en Historia Clínica, junto con la documentación aportada (bibliografía, informe de servicio o departamento implicado, informes de otras comisiones que se consideren pertinentes,...), debe ser presentada por el Jefe de Servicio o el Coordinador de Calidad del mismo, dirigiéndola al presidente o secretario de la Comisión de Documentación Clínica.

La solicitud será valorada por la Comisión de Documentación Clínica, desde donde se elaborará el informe correspondiente. En caso de no aportar documentación suficiente, será requerida previa al estudio.

En caso de que el informe sea desfavorable, se remitirá debidamente detallado al Servicio que inició el procedimiento para que sean consideradas, si es el caso, las indicaciones de la Comisión y se inicie de nuevo el proceso.

En caso de que el informe sea favorable, se remitirá a la Dirección correspondiente para su valoración y comienzo del siguiente proceso, que concluye en este caso con las instrucciones pertinentes para su modelaje y reprografía o en su momento su inclusión en la historia clínica electrónica según el procedimiento que en su momento se decida para ello.

Responsabilidades.

La Comisión de Documentación clínica tiene entre otras, las funciones de:

- Velar por la veracidad y confidencialidad de los datos incluidos en los registros clínico-administrativos, en todas sus formas de presentación, redactando y difundiendo las normas que se consideren necesarias para tal fin.
- Definir los procesos y establecer los procedimientos para el uso de la documentación y registros clínico-administrativos y de la información desprendida de los mismos.
- Contribuir a la mejora continua de la calidad de la Historia Clínica y Registros clínico-administrativos, colaborando además con los programas institucionales y del propio hospital en los temas relacionados.
- Evaluar los documentos de registro de actividad clínica contribuyendo a su normalización y participando en el diseño de los mismos.

De acuerdo a estas líneas, a la hora de emitir un informe favorable, se tendrán en cuenta:

- Alineamiento con la política del Hospital en cuanto a documentación clínica se refiere.
- Bibliografía y documentación aportada.
- Factibilidad de su inclusión y utilización posterior.
- Contribución a la mejora de la Historia Clínica y sus registros.

Registros.

El procedimiento para el registro, se incluirá en la Guía de Documentación Clínica del Hospital.

Impresos.

El informe emitido por la Comisión, incluirá el modelo de impreso normalizado propuesto, "o el formulario propuesto para evaluación y realización por la comisión u organismo que se determine en el seno del funcionamiento de la historia clínica electrónica", con objeto de que se tenga en cuenta por parte de la Dirección correspondiente a la hora de gestionar la provisión y distribución de los mismos.

Lista de distribución.

Este procedimiento y sus sucesivas actualizaciones, será incluido en la Guía de Documentación Clínica del Hospital, además de ser enviado a todas las Direcciones Asistenciales, a los distintos Jefes de Servicio y a los Coordinadores de Calidad.

La forma de envío será a través del correo electrónico, conservándose el justificante del envío (impresión del e-mail enviado junto con las direcciones a las que se le ha remitido).

Revisión.

El presente documento será revisado y actualizado por la comisión de documentación con una periodicidad máxima de 4 años, y sin falta se realizará una revisión para adecuar este documento a la nueva historia clínica electrónica tras la implantación de la misma.

Anexo [II] Solicitud de rectificación o cancelación de datos sanitarios, ejemplo en un hospital del Servicio Madrileño de Salud

Instituto Psiquiátrico Servicio de Salud Mental José Germain	SOLICITUD DE RECTIFICACIÓN O CANCELACIÓN DE DATOS SANITARIOS	CÓDIGO: PAD-FL-09
		VERSIÓN: 1

CENTRO DE SALUD (Poner nombre del centro): _____

DATOS DEL SOLICITANTE:

Nombre y Apellidos: _____

Documento que acredite identidad: (DNI, NIE, Pasaporte...) (*): _____

Domicilio: _____

Código Postal: _____ Localidad: _____

Teléfono de contacto móvil: _____ Teléfono de contacto fijo: _____

SOLICITO EN CALIDAD DE: (Marcar la opción correspondiente y **acreditar identidad y representación**):

☐ Titular de la Historia Clínica

☐ Representante Legal (Menor, incapacitado....)

☐ Representante voluntario.

TITULAR DE HISTORIA CLÍNICA Fecha de Nacimiento: _____

Nombre y Apellidos: _____ DNI_____

TIPO DE SOLICITUD (Marcar la opción correspondiente):

☐ Rectificación de datos

☐ Cancelación de datos

DATO A RECTIFICAR O CANCELAR: _____

DOCUMENTACIÓN QUE APORTA _____

_____

Madrid a _____de _____ de 20__

Firma del solicitante

(*) Debe de acreditar su identidad al personal del Centro que lo solicite.
(**) En caso de autorizar a otra personal a retirar la documentación, debe acompañar fotocopia del DNI que acredite la identidad del titular de la documentación clínica.

Red H s H

Pág. 1 de 2

Instituto Psiquiátrico Servicios de Salud Mental José Germain	SOLICITUD DE RECTIFICACIÓN O CANCELACIÓN DE DATOS SANITARIOS	CÓDIGO: PAD-FL-09
		VERSIÓN: 1

CENTRO DE SALUD (Poner nombre del centro): _____

DATOS DEL SOLICITANTE:

Nombre y Apellidos: _____

Documento que acredite identidad: (DNI, NIE, Pasaporte...) (*): _____

Domicilio: _____

Código Postal: _____ Localidad: _____

Teléfono de contacto móvil: _____ Teléfono de contacto fijo: _____

SOLICITO EN CALIDAD DE: (Marcar la opción correspondiente y **acreditar identidad y representaoión**):

☐ Titular de la Historia Clínica

☐ Representante Legal (Menor, Incapacitado....)

☐ Representante voluntario.

TITULAR DE HISTORIA CLÍNICA Fecha de Nacimiento: _____

Nombre y Apellidos: _____ DNI_____

TIPO DE SOLICITUD (Marcar la opción correspondiente):

☐ Rectificación de datos

☐ Cancelación de datos

DATO A RECTIFICAR O CANCELAR: _____

DOCUMENTACIÓN QUE APORTA _____

_____

Madrid a _____de _____ de 20__

Firma del solicitante

(*) Debe de acreditar su identidad al personal del Centro que lo solicite.
(**) En caso de autorizar a otra personal a retirar la documentación, debe acompañar fotocopia del DNI que acredite la identidad del titular de la documentación clínica.

Red H s H

Pág. 1 de 2

Anexo JJ Informe sobre los tratamientos de datos en relación con el COVID-19. Agencia Española de Protección de Datos

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.*

Por lo tanto, como base jurídica para un tratamiento lícito de datos personales, sin perjuicio de que puedan existir otras bases, -como por ejemplo el cumplimiento de una obligación legal, art. 6.1.c) RGPD (para el empleador en la prevención de riesgos laborales de sus empleados)-, el RGPD reconoce explícitamente las dos citadas: misión realizada en interés público (art. 6.1.e) o intereses vitales del interesado u otras personas físicas (art. 6.1.d).

El art. 6.1, letra d) RGPD considera no sólo que el interés vital es suficiente base jurídica del tratamiento para proteger al "interesado" (en cuanto que este es un término definido en el art. 4.1) RGPD como persona física identificada o identificable), sino que dicha base jurídica puede ser utilizada para proteger los intereses vitales "de otra persona física", lo que por extensión supone que dichas personas físicas pueden ser incluso no identificadas o identificables; es decir, dicha base jurídica del tratamiento (el interés vital) puede ser suficiente para los tratamientos de datos personales dirigidos a proteger a todas aquellas personas susceptibles de ser contagiadas en la propagación de una epidemia, lo que justificaría, desde el punto de vista de tratamiento de datos personales, en la manera más amplia posible, las medidas adoptadas a dicho fin, incluso aunque se dirijan a proteger personas innominadas o en principio no identificadas o identificables, por cuanto los intereses vitales de dichas personas físicas habrán de ser salvaguardados, y ello es reconocido por la normativa de protección de datos personales.

El apartado 3 del artículo 6 RGPD no establece la necesidad de que la base del tratamiento por razón de interés vital haya de ser establecida por el Derecho de la Unión o el Derecho de los Estados Miembros aplicables al responsable del tratamiento, pues dicho apartado se refiere exclusivamente a los tratamientos establecidos para el cumplimiento de una obligación legal, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, ambas referidas en las letras c) y e) de dicho artículo 6 RGPD, pero no para los tratamientos incluidos en la letra d).

Sin embargo, para el tratamiento de datos de salud no basta con que exista una base jurídica del art. 6 RGPD, sino que de acuerdo con el art. 9.1 y 9.2 RGPD exista una circunstancia que levante la prohibición de tratamiento de dicha categoría especial de datos (entre ellos, datos de salud).

Esta AEPD entiende que dichas circunstancias cabe encontrarlas, en este caso, en varios de los epígrafes del art. 9.2 RGPD. Así:

(I) En la letra b), en las relaciones ente empleador y empleado, por cuanto el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento (el empleador) o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, ya que el empleador está sujeto o a la normativa de prevención de riesgos laborales (Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales) de la cual se desprende, artículo 14 y concordantes de dicha ley, un deber del empresario de protección de los trabajadores frente a los riesgos laborales, para lo cual el empresario deberá garantizar la seguridad y salud de todos los trabajadores a su servicio en los aspectos relacionados con el trabajo. Por ese mismo fundamento, el art. 29 de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales, que transpone el art. 13 de la Directiva del Consejo (89/391/CEE), de 12 de junio de 1989, relativa a la aplicación de medidas para promover la mejora de la seguridad y de la salud de los trabajadores en el trabajo, establece también obligaciones de los trabajadores en materia de prevención de riesgos. Así, corresponde a cada trabajador velar, según sus posibilidades y mediante el cumplimiento de las medidas de prevención que en cada caso sean adoptadas, por su propia seguridad y salud en el trabajo y por la de aquellas otras personas a las que pueda afectar su actividad profesional, a causa de sus actos y omisiones en el trabajo, de conformidad con su formación y las instrucciones del empresario. Ello se concreta en que deberán de informar de inmediato a su superior jerárquico directo, y a los trabajadores designados para realizar actividades de protección y de prevención o, en su caso, al servicio de prevención, acerca de cualquier situación que, a su juicio, entrañe, por motivos razonables, un riesgo para la seguridad y la salud de los trabajadores; contribuir al cumplimiento de las obligaciones establecidas por la autoridad competente con el fin de proteger la seguridad y la salud de los trabajadores en el trabajo y cooperar con el empresario para que éste pueda garantizar unas condiciones de trabajo que sean seguras y no entrañen riesgos para la seguridad y la salud de los trabajadores. En el ámbito de la situación actual derivada del covid-19 ello supone que el trabajador deberá informar a su

empleador en caso de sospecha de contacto con el virus, a fin de salvaguardar, además de su propia salud, la de los demás trabajadores del centro de trabajo, para que se puedan adoptar las medidas oportunas. El empleador deberá tratar dichos datos conforme al RGPD, debiendo adoptarse las medidas oportunas de seguridad y responsabilidad proactiva que demanda el tratamiento (art. 32 RGPD).

(II) En la letra g), y en la i), que pueden ser examinadas conjuntamente, por cuanto ambas hacen referencia a un interés público, el primero de ellos calificado de "esencial" y el segundo de ellos que hace referencia a un interés público calificado "en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud", todo ello sobre la base del Derecho de la Unión o de los Estados Miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional

(III) En la letra h), cuando el tratamiento es necesario para realizar un diagnóstico médico, o evaluación de la capacidad de laboral del trabajador o cualquier otro tipo de asistencia de tipo sanitario o para la gestión de los sistemas y servicios de asistencia sanitaria y social.

(IV) Una última circunstancia de cierre que permitiría el tratamiento de datos de salud podría ser incluso la establecida en la letra c), en el caso de que se den las circunstancias previstas en este apartado, que aplicaría cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

Dentro de estos criterios, por lo tanto, el RGPD ha pretendido dar la mayor libertad posible a los responsables del tratamiento en caso de necesidad para salvaguardar intereses vitales de los interesados o de otras personas físicas, intereses públicos esenciales en el ámbito de la salud pública o cumplimiento de obligaciones legales, dentro de las medidas establecidas en la normativa legal correspondiente del Estado miembro o de la Unión Europea en cada caso aplicable.

II

En consecuencia, en una situación de emergencia sanitaria como a la que se refiere la solicitud de este informe, es preciso tener en cuenta que, en el exclusivo ámbito de la normativa de protección de datos personales, la

agencia española protección datos

Gabinete Jurídico

N/REF: 0017/2020

Examinada su solicitud de informe, en relación con los tratamientos de datos resultantes de la actual situación derivada de la extensión del virus COVID-19, en primer lugar, con carácter general, debe aclararse que la normativa de protección de datos personales, en tanto que dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual, dado que no existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada.

Sin perjuicio de lo anterior, la propia normativa de protección de datos personales (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, RGPD) contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe una emergencia sanitaria de alcance general. Por ello, al aplicarse dichos preceptos previstos para estos casos en el RGPD, en consonancia con la normativa sectorial aplicable en el ámbito de la salud pública, las consideraciones relacionadas con la protección de datos -dentro de los límites previstos por las leyes- 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.

I

El Considerando (46) del RGPD ya reconoce que en situaciones excepcionales, como una epidemia, la base jurídica de los tratamientos puede ser múltiple, basada tanto en el interés público, como en el interés vital del interesado u otra persona física.

> *(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra*

c. Jorge Juan 6
28001 Madrid
www.aepd.es

aplicación de la normativa de protección de datos personales permitiría adoptar al responsable del tratamiento aquellas decisiones que sean necesarias para salvaguardar los intereses vitales de las personas físicas, el cumplimiento de obligaciones legales o la salvaguardia de intereses esenciales en el ámbito de la salud pública, dentro de lo establecido por la normativa material aplicable.

Cuáles sean dichas decisiones, (desde el punto de vista de la normativa de protección de datos personales, se reitera) serán aquellas que los responsables de los tratamientos de datos deban de adoptar conforme a la situación en que se encuentren, siempre dirigida a salvaguardar los intereses esenciales ya tan reiterados. Pero los responsables de tratamientos, al estar actuando para salvaguardar dichos intereses, deberán actuar conforme a lo que las autoridades establecidas en la normativa del Estado miembro correspondiente, en este caso España, establezcan.

Así, el legislador español se ha dotado de las medidas legales necesarias oportunas para enfrentarse a situaciones de riesgo sanitario, como la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, publicado en el Boletín Oficial del Estado de 11 de marzo de 2020) o la Ley 33/2011, de 4 de octubre, General de Salud Pública. El artículo 3 de la primera de dichas normas señala que:

> *[c]on el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato,* ***así como las que se consideren necesarias en caso de riesgo de carácter transmisible****.*

Del mismo modo, los artículos 5 y 84 de la Ley 33/2011, de 4 de octubre, General de Salud Pública se refieren a la anterior Ley orgánica 3/1986, y a la posibilidad de adoptar medidas adicionales en caso de riesgo de transmisión de enfermedades.

Por lo tanto, en materia de riesgo de transmisión de enfermedades, epidemia, crisis sanitarias etc., la normativa aplicable ha otorgado "a las autoridades sanitarias de las distintas Administraciones públicas" (art. 1 Ley Orgánica 3/1986, de 14 de abril) las competencias para adoptar las medidas

necesarias previstas en dichas leyes cuando así lo exijan razones sanitarias de urgencia o necesidad.

En consecuencia, desde un punto de vista de tratamiento de datos personales, la salvaguardia de intereses esenciales en el ámbito de la salud pública corresponde a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las medidas necesarias para salvaguardar dichos intereses esenciales públicos en situaciones de emergencia sanitaria de salud pública.

Serán estas autoridades sanitarias competentes de las distintas administraciones públicas quienes deberán adoptar las decisiones necesarias, y los distintos responsables de los tratamientos de datos personales deberán seguir dichas instrucciones, incluso cuando ello suponga un tratamiento de datos personales de salud de personas físicas. Lo anterior hace referencia, expresamente, a la posibilidad de tratar los datos personales de salud de determinadas personas físicas por los responsable de tratamientos de datos personales, cuando, por indicación de las autoridades sanitarias competentes, es necesario comunicar a otras personas con las que dicha persona física ha estado en contacto la circunstancia del contagio de esta, para salvaguardar tanto a dichas personas físicas de la posibilidad de contagio (intereses vitales de las mismas) cuanto para evitar que dichas personas físicas, por desconocimiento de su contacto con un contagiado puedan expandir la enfermedad a otros terceros (intereses vitales de terceros e interés público esencial y/o cualificado en el ámbito de la salud pública).

Del mismo modo, y en aplicación de lo establecido en la normativa de prevención de riesgos laborales, y de medicina laboral, los empleadores podrán tratar, de acuerdo con dicha normativa y con las garantías que estas normas establecen, los datos de sus empleados necesarios para garantizar la salud de todos sus empleados, lo que incluye igualmente al resto de empleados distintos del interesado, para asegurar su derecho a la protección de la salud y evitar contagios en el seno de la empresa y/o centros de trabajo.

III

Ahora bien, los tratamientos de datos personales en estas situaciones de emergencia sanitaria, como se ha mencionado al principio de este informe, siguen siendo tratados de conformidad con la normativa de protección de datos personales (RGPD y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LOPDGDD), por lo que

se aplican todos sus principios, contenidos en el artículo 5 RGPD, y entre ellos el de tratamiento de los datos personales con licitud, lealtad y transparencia, de limitación de la finalidad (en este caso, salvaguardar los intereses vitales/esenciales de las personas físicas), principio de exactitud, y por supuesto, y hay que hacer especial hincapié en ello, el principio de minimización de datos. Sobre este último aspecto hay que hacer referencia expresa a que los datos tratados habrán de ser exclusivamente los limitados a los necesarios para la finalidad pretendida, sin que se pueda extender dicho tratamiento a cualesquiera otros datos personales no estrictamente necesarios para dicha finalidad, sin que pueda confundirse conveniencia con necesidad, porque el derecho fundamental a la protección de datos sigue aplicándose con normalidad, sin perjuicio de que, como se ha dicho, la propia normativa de protección de datos personales establece que en situaciones de emergencia, para la protección de intereses esenciales de salud pública y/o vitales de las personas físicas, podrán tratarse los datos de salud necesarios para evitar la propagación de la enfermedad que ha causado la emergencia sanitaria. Respecto del principio de limitación de la finalidad en relación con supuestos de tratamientos de datos de salud por razones de interés público, el Considerando (54) RGPD es claro, cuando establece que:

> *El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. […] Este tratamiento de datos relativos a la salud por razones de interés público* ***no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines***.

Anexo [KK] Procedimiento de detección del nuevo coronavirus SARS-CoV-2 en la Comunidad de Madrid. Red de Vigilancia Epidemiológica de la Comunidad de Madrid

Comunidad de Madrid

Dirección General de Salud Pública
CONSEJERÍA DE SANIDAD

PROCEDIMIENTO DE DETECCIÓN DEL NUEVO CORONAVIRUS SARS-CoV-2 EN LA COMUNIDAD DE MADRID

Febrero 2020

Elaborado por los Servicios de Microbiología de los Hospitales 12 de Octubre, La Paz, Ramón y Cajal, Gregorio Marañón y la Dirección General de Salud Pública.

1. INTRODUCCIÓN

Ante la identificación en diciembre de 2019 de un brote de neumonía en China causado por un nuevo Coronavirus (betaCoronavirus) capaz de transmitirse entre humanos, denominado SARS-CoV-2, no se puede descartar que aparezca algún caso importado en España procedente de la zona de riesgo. Todo caso que cumpla los criterios de **caso en investigación** requiere el estudio microbiológico de la infección por SARS-CoV-2 en un laboratorio que disponga de las técnicas específicas para la realización de este diagnóstico mediante PCR.

Con el objeto de reducir el tiempo de respuesta para la confirmación de un caso en investigación, la Comunidad de Madrid propone que los servicios de Microbiología de los Hospitales 12 de Octubre, Ramón y Cajal, La Paz y Gregorio Marañón organicen una red preparada para atender las solicitudes diagnósticas que se hagan desde la Dirección General de Salud Pública.

Todas las muestras deben proceder de pacientes que, tras la evaluación de Salud Pública, cumplan los criterios de caso en investigación. La Dirección General de Salud Pública autorizará el envío de muestras.

Las definiciones utilizadas en este protocolo están incluidas en el Procedimiento de Actuación frente a casos de infección por el nuevo Coronavirus (SARS-CoV-2) adaptado a la Comunidad de Madrid[1].

En el anexo 1 se puede consultar la distribución de los hospitales según derivación de muestras para estudio de infección por SARS-CoV-2.

2. OBJETIVO Y ÁMBITO DE APLICACIÓN

El objetivo del presente documento es describir el proceso a seguir para el diagnóstico de la infección por el nuevo Coronavirus en los Servicios de Microbiología de los Centros Hospitalarios de la Comunidad de Madrid.

3. PRINCIPIO DEL MÉTODO

El método diagnóstico se basa en la detección del ARN viral presente en las muestras clínicas de los pacientes infectados. Para ello se utilizará una técnica de RT-PCR en tiempo real que detectará 2 regiones del genoma viral: gen E (genérico de Sarbecovirus: SARS) y gen RdRP (especifico de SARS-CoV-2) [procedimiento descrito en Corman VM et al. Detection of 2019 novel coronavirus (SARS-CoV-2) by real-time RT-PCR. Euro Surveill. 2020;25(3):pii=2000045].

4. TIPO DE MUESTRA QUE DEBE SER REMITIDO AL SERVICIO DE MICROBIOLOGIA

Muestras del tracto respiratorio:

a. Superior*: exudado nasofaríngeo/orofaríngeo en pacientes ambulatorios.

y

b. Inferior: preferentemente lavado broncoalveolar, esputo (si es posible) y/o aspirado endotraqueal especialmente en pacientes con enfermedad respiratoria grave.

**En pacientes pediátricos se contemplará la toma de aspirados nasofaríngeos*

[1] *Procedimiento de actuación frente a casos de infección por el nuevo coronavirus (SARS-COV2) adaptado a la Comunidad de Madrid*

NOTA:

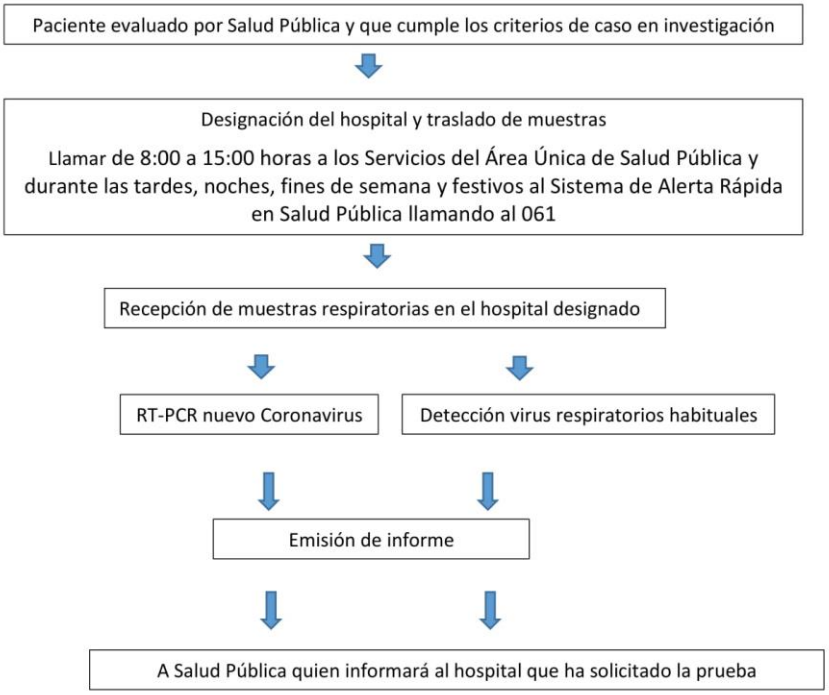
Si un paciente no tiene signos o síntomas de infección del tracto respiratorio inferior o si la toma de muestras del tracto respiratorio inferior está clínicamente indicada, pero no es posible su recolección, se puede optar por estudiar SÓLO las muestras respiratorias de tracto superior.

Si las pruebas iniciales son negativas en un paciente con una alta sospecha clínica y epidemiológica para SARS-CoV-2 (especialmente cuando solo se han recogido muestras de tracto respiratorio superior o la muestra recogida inicialmente no estaba tomada adecuadamente) se repetirá el diagnóstico con nuevas muestras del tracto respiratorio. Se podrán extraer muestras adicionales como sangre, orina o heces.

5. MATERIALES

Los 4 hospitales designados cuentan con todo el equipamiento necesario para la realización de esta técnica diagnóstica. Así mismo los 4 centros realizan, tanto en rutina como de forma urgente, la detección molecular de los virus respiratorios habituales.

6. PROCEDIMIENTO Y ESQUEMA DE TRABAJO



6.1. Solicitud de la prueba

Cada centro adecuará la solicitud de la determinación del nuevo Coronavirus a su sistema informático (SIL) y a la historia clínica electrónica vigente.

Todas las muestras deben de proceder de pacientes evaluados por Salud Pública y que cumplan los criterios de caso en investigación.

La solicitud se realizará de 8:00 a 15:00 horas a los Servicios del Área Única de Salud Pública y durante las tardes, noches, fines de semana y festivos al Sistema de Alerta Rápida en Salud Pública llamando al 061. Desde Salud Pública se darán las indicaciones oportunas para el tranporte de la muestra según el centro.

La asignación para la derivación de muestras, desde los hospitales de la red sanitaria tanto pública como privada, a los hospitales designados para la realización de PCR, se ha realizado siguiendo criterios geográficos y organizativos.

Normas de bioseguridad

Las muestras serán enviadas al laboratorio en un embalaje de bioseguridad categoría B (triple envoltorio). Para el procesamiento de las muestras se utilizarán los equipos de protección individual (bata, mascarilla FFP2, gafas y guantes) recomendados en cada centro por el Servicio de Prevención de Riesgos Laborales. El procesamiento inicial y la inactivación de las muestras se realizará en cabina de seguridad biológica de clase II.

6.2. Recepción de las muestras

Las muestras procedentes del propio centro hospitalario serán remitidas al Servicio de Microbiología de acuerdo a las instrucciones indicadas en el protocolo local de cada Hospital. Y para la recepción de las muestras procedentes de otros Centros Hospitalarios se seguirán las instrucciones de Salud Pública.

6.3. Preparación de las muestras a su llegada al laboratorio designado (debe realizarse en cabina de seguridad biológica tipo II)

- Los exudados nasofaríngeos serán vorteados
- Los aspirados nasofaríngeos y los LBAs serán diluidos en una proporción 1:1 con medio de dilución (UTM)
- Las secreciones respiratorias (esputos, aspirados) serán homogeneizadas siguiendo los protocolos habituales para el procesamiento de este tipo de muestras en cada Centro
- Antes de proceder a la extracción las muestras serán **INACTIVADAS**, realizando un proceso de lisis con tal fin (utilización de reactivos comerciales que contengan isotiocianato de guanidina a concentraciones adecuadas)
- Se utilizarán las plataformas de extracción disponibles en cada Centro, y que ya se vienen utilizando para la obtención del material genómico de otros virus respiratorios
- Como ya se ha indicado todos los Centros realizarán la detección simultánea de dos regiones del genoma: gen E y gen RdRP
- El tiempo de respuesta estimado desde la recepción de la muestra es inferior a 4 horas.

6.4. Emisión de informes e interpretación de los resultados

En el informe de resultados que se emita debe incluirse la confirmación del caso (amplificación de las 2 regiones del genoma viral)

Resultado: Detección POSITIVA del Nuevo Coronavirus SARS-CoV-2

Resultado: Detección NEGATIVA del Nuevo Coronavirus SARS-CoV-2

Resultado*: Se solicita una nueva muestra para realizar la detección de SARS-CoV-2*

**En caso de amplificación de una sola diana. En este último caso debe solicitarse la obtención de otra muestra, preferentemente del tracto respiratorio inferior.*

Cada uno de los centros designados emitirá el informe de resultados de la determinación del nuevo Coronavirus según su sistema informático (SIL) o en otro formato que considere oportuno.

El resultado se enviará a Salud Pública por correo electrónico y mediante llamada telefónica. Una vez recibido el informe de resultados, Salud Pública informará del mismo al Hospital que ha solicitado la prueba. El Centro que envíe la muestra a cualquiera de los Hospitales de referencia debe indicar correo electrónico y teléfono de contacto junto a los datos básicos del paciente en investigación para poder realizar el registro informático de la petición y de sus resultados. Los datos de filiación del paciente incluirán el CIPA si lo tiene.

7. ASEGURAMIENTO DE LA CALIDAD

La técnica de amplificación debe incluir controles internos que garanticen la eficacia tanto del proceso de extracción de ácidos nucleicos como de amplificación.

Para el aseguramiento externo de la calidad las muestras evaluadas serán remitidas al Centro Nacional de Microbiología para su posterior evaluación.

ANEXO. Datos de contacto con la Dirección General de Salud Pública

Servicios del Área Única de Salud Pública

Servicio del Área Única de Salud Pública-1,4,7
Servicio del Área Única de Salud Pública-2
Servicio del Área Única de Salud Pública-3
Servicio del Área Única de Salud Pública-5
Servicio del Área Única de Salud Pública-6
Servicio del Área Única de Salud Pública-8
Servicio del Área Única de Salud Pública-9
Servicio del Área Única de Salud Pública-10
Servicio del Área Única de Salud Pública-11

Tabla resumen direcciones postales y teléfonos

	Dirección	Teléfono	Fax
AREA ÚNICA DE SALUD PÚBLICA 1	C/ Cincovillas, 5 (28051 MADRID)	91 494 24 79	91 494 07 19
AREA ÚNICA DE SALUD PÚBLICA 2	C/ Océano Pacífico, 3 (28821 COSLADA)	91 672 32 18	91 673 85 15
AREA ÚNICA DE SALUD PÚBLICA 3	Avda. Reyes Magos, s/n (28806 ALCALÁ DE HENARES)	91 880 60 07	91 882 84 06
AREA ÚNICA DE SALUD PÚBLICA 4	C/ Cincovillas, 5 (28051 MADRID)	91 494 24 79	91 494 07 19
AREA ÚNICA DE SALUD PÚBLICA 5	C/ Blas de Otero 13 – 3ª planta (28100 ALCOBENDAS)	91 490 41 10	91 661 42 96
AREA ÚNICA DE SALUD PÚBLICA 6	C/ Aristóteles, 3 (28230 LAS ROZAS DE MADRID)	91 227 69 00	91/ 204 38 26
AREA ÚNICA DE SALUD PÚBLICA 7	C/ Cincovillas, 5 (28051 MADRID)	91 494 24 79	91 494 07 19
AREA ÚNICA DE SALUD PÚBLICA 8	C/ Alonso Cano 8 (28933 MÓSTOLES)	91 621 10 40	91/ 811 32 56
AREA ÚNICA DE SALUD PÚBLICA 9	Avda. Portugal 2 - 1ª planta (28916 LEGANÉS)	91 248 49 00	91/ 686 38 11
AREA ÚNICA DE SALUD PÚBLICA 10	C/ Alberto Palacios 22 (28021 MADRID)	91 696 41 66	91/ 696 63 51
AREA ÚNICA DE SALUD PÚBLICA 11	C/ Alberto Palacios 22 (28021 MADRID)	91 710 96 67	91/ 798 01 32
Servicio de Epidemiología	C/ San Martín de Porres 6 – 1ª planta (28035 MADRID)	91 370 08 88	91 370 08 83
Servicio de Alertas en Salud Pública	C/ San Martín de Porres 6 – 1ª planta (28035 MADRID)	91 370 08 03	91 370 08 09

Anexo [LL] Comunicación de la ViceConsejería de Sanidad de la Comunidad de Madrid, el día 27 de abril de 2018, a la Agencia Española de Protección de Datos la creación de una figura colegiada denominada Comité delegado de protección de datos

Comunidad de Madrid

Viceconsejería de Sanidad
Servicio Madrileño de Salud
CONSEJERÍA DE SANIDAD

A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

D. Manuel Molina Muñoz, Consejero de Sanidad de la Comunidad de Madrid según nombramiento mediante Decreto 104/2015, de 7 de julio, del Consejo de Gobierno, y actuando en nombre y representación de la Consejería de Sanidad ante la Agencia Española de Protección de Datos comparezco y como mejor proceda,

DIGO

Que por medio del presente escrito, vengo a comunicar a la Agencia Española de Protección de Datos, dentro del plazo legal establecido, los datos correspondientes al Delegado de Protección de Datos de la Consejería de Sanidad de la Comunidad de Madrid (en adelante CSCM), que revestirá la forma de Comité. Todo ello en cumplimiento de lo estipulado en los artículos art. 37.1.a y 37.7 del RGPD en función de la condición de organismo público de la Consejería a la que represento.

Que el **Comité de Seguridad de la Información de la CSCM**, en reunión celebrada en Madrid el día 2 de marzo de 2018, acordó, en virtud de sus competencias según Orden 491/2013, de 27 de junio, de la Consejería de Sanidad, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica y de los sistemas de información de la Consejería de Sanidad de la Comunidad de Madrid (BOCM de 18 de julio de 2013), el nombramiento del Delegado de Protección de Datos de la Consejería de Sanidad en la figura colegiada del **Comité Delegado de Protección de Datos**, con la siguiente composición:

- Presidente: el titular de la Subdirección General de Innovación y Arquitectura Tecnológica de la CSCM. Actualmente, D. David Lleras Iglesias (Resolución de 2 de junio de 2014, BOCM nº 141, de 16 de junio)
- Vocal-Secretario: el responsable de Seguridad de Sistemas de Información Sanitaria de la CSCM. Actualmente, D. José Manuel Laperal González

Se atribuye al Vocal-Secretario la función de interlocutor con la Agencia Española de Protección de Datos. Se atribuye al Presidente del Comité DPD de la CSCM la facultad de nombrar vocales, así como otros componentes del Comité en funciones de asesoría legal y/o técnica.

Edificio Sollube
Plaza Carlos Trías Bertrán, 7
28020- Madrid

En virtud de lo anterior,

SOLICITO

Que se tenga por presentada la designación del Comité DPD de la CSCM, el cual adopta las funciones que la legislación vigente le encomienda.

En Madrid, 27 de abril de 2018

Fdo. EL VICECONSEJERO DE SANIDAD DE LA COMUNIDAD DE MADRID

D. Manuel Molina Muñoz

Edificio Sollube
Plaza Carlos Trías Bertrán, 7
28020- Madrid

Dirección General de Sistemas de Información Sanitaria
SERVICIO MADRILEÑO DE SALUD
CONSEJERÍA DE SANIDAD

OSSI

DELEGADO DE PROTECCIÓN DE DATOS: ESTRUCTURA Y FUNCIONES

Por tratarse de una entidad que forma parte de la Administración Pública que de manera habitual y sistemática trata datos personales de categoría especial de interesados a gran escala, la Consejería de Sanidad se ha visto en la obligación de designar un Delegado de Protección de Datos, como bien le exige la normativa en esta materia, en específico lo dispuesto en los artículos 37.1.a) del *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD).*

En virtud de su estructura organizativa, la Consejería de Sanidad ha adoptado la forma de Comité Delegado de Protección de Datos, el cual está integrado por los siguientes miembros:

- **Un Presidente**, asumiendo esta función el Subdirector General de Planificación e Innovación de la Dirección General del Sistemas de Información Sanitaria.

- **Un Secretario**, asumiendo esta función el Responsable de Seguridad de Sistemas de Información Sanitaria de la Dirección General Sistemas de Información del Servicio Madrileño de Salud.

- **Un Organismo Asesor**, asumiendo esta función la Oficina de Seguridad de Sistemas de Información Sanitaria (OSSI), entidad externa que se encuentra al servicio de la Dirección General de Sistemas de Información.

Acorde al contenido de dicha normativa, el Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

1. Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

2. Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

3. Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.

4. Cooperar con la autoridad de control;

5. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Anexo [MM] Distribución de los Centros de Salud y Consultorios Locales del SERMAS en la Comunidad de Madrid a fecha de 31/05/2021 según Disponible en https://www.comunidad.madrid/servicios/salud/atencion-primaria

Dirección asistencial Norte

- ALCOBENDAS
  - C.S. ARROYO DE LA VEGA
  - C.S. LA CHOPERA
  - C.S. MARQUÉS DE LA VALDAVIA
  - C.S. MIRAFLORES
  - C.S. VALDELASFUENTES
- ALGETE
  - C.S. ALGETE
    - C.L. ALALPARDO
    - C.L. COBEÑA
    - C.L. FUENTE EL SAZ
    - C.L. SANTO DOMINGO (Urb.)
    - C.L. TALAMANCA
    - C.L. VALDEOLMOS
    - C.L. VALDEPIÉLAGOS
    - C.L. VALDETORRES
- BUITRAGO DE LOZOYA
  - C.S. BUITRAGO DE LOZOYA
    - C.L. AOSLOS
    - C.L. BERZOSA DEL LOZOYA
    - C.L. BOCIGANO
    - C.L. BRAOJOS
    - C.L. CABIDA
    - C.L. CANENCIA
    - C.L. CERVERA DE BUITRAGO
    - C.L. CINCOVILLAS
    - C.L. COLMENAR DE LA SIERRA
    - C.L. CORRALEJO
    - C.L. EL CARDOSO
    - C.L. GANDULLAS
    - C.L. GARGANTA DE LOS MONTES
    - C.L. GARGANTILLA DEL LOZOYA
    - C.L. GASCONES
    - C.L. HORCAJO DE LA SIERRA
    - C.L. HORCAJUELO DE LA SIERRA
    - C.L. LA ACEBEDA
    - C.L. LA HIRUELA
    - C.L. LA SERNA DEL MONTE
    - C.L. MADARCOS
    - C.L. PIÑUÉCAR
    - C.L. PRÁDENA DEL RINCÓN
    - C.L. PUEBLA DE LA SIERRA
    - C.L. ROBLEDILLO DE LA JARA
    - C.L. ROBREGORDO
    - C.L. SAN MAMÉS
    - C.L. SERRADA DE LA FUENTE
    - C.L. SOMOSIERRA
    - C.L. VILLAVIEJA DEL LOZOYA
- COLMENAR VIEJO
  - C.S. COLMENAR VIEJO NORTE
  - C.S. COLMENAR VIEJO SUR
- EL MOLAR
  - C.S. EL MOLAR
    - C.L. COTOS DE MONTERREY
    - C.L. EL ESPARTAL
    - C.L. EL VELLÓN
    - C.L. PEDREZUELA
    - C.L. REDUEÑA
    - C.L. SAN AGUSTÍN DE GUADALIX
    - C.L. VENTURADA
- LA CABRERA
  - C.S. LA CABRERA
    - C.L. CABANILLAS
    - C.L. EL BERRUECO
    - C.L. EL CUADRÓN
    - C.L. LAS NAVAS DE BUITRAGO
    - C.L. LOZOYUELA
    - C.L. SIETEIGLESIAS
    - C.L. VALDEMANCO
- MADRID
  - C.S. BARRIO DEL PILAR
  - C.S. BUSTARVIEJO
  - C.S. CIUDAD PERIODISTAS
  - C.S. DR. CASTROVIEJO
  - C.S. FUENCARRAL
  - C.S. FUENTELARREINA
  - C.S. INFANTA MERCEDES
  - C.S. JOSÉ MARVÁ
  - C.S. LA VENTILLA
  - C.S. MIRASIERRA
  - C.S. NÚÑEZ MORGADO
  - C.S. REINA VICTORIA
  - C.S. VILLAAMIL
  - C.S. VIRGEN DE BEGOÑA
- MANZANARES EL REAL
  - C.S. MANZANARES EL REAL
    - C.L. CERCEDA
    - C.L. EL BOALO
    - C.L. MATALPINO
- PARACUELLOS DEL JARAMA
  - C.S. PARACUELLOS de JARAMA
    - C.L. AJALVIR
    - C.L. BELVIS DEL JARAMA
    - C.L. DAGANZO DE ARRIBA
    - C.L. RIBATEJADA
    - C.L. SERRACINES
- RASCAFRIA
  - C.S. RASCAFRÍA
    - C.L. ALAMEDA DEL VALLE
    - C.L. LOZOYA DEL VALLE
    - C.L. OTERUELO
    - C.L. PINILLA DEL VALLE
- SAN SEBASTIÁN DE LOS REYES
  - C.S. REYES CATÓLICOS
  - C.S. ROSA LUXEMBURGO
  - C.S. V CENTENARIO
- SOTO DEL REAL
  - C.S. SOTO DEL REAL
    - C.L. BUSTARVIEJO
    - C.L. GUADALIX DE LA SIERRA
    - C.L. MIRAFLORES DE LA SIERRA
    - C.L. NAVALAFUENTE
- TORRELAGUNA
  - C.S. TORRELAGUNA
    - C.L. EL ATAZAR
    - C.L. PATONES
    - C.L. TORREMOCHA DEL JARAMA
- TRES CANTOS
  - C.S. SECTOR EMBARCACIONES
    - C.S. TRES CANTOS

1

Dirección asistencial Este

ALCALÁ DE HENARES
- C.S. CARMEN CALZADO
- C.S. JUAN DE AUSTRIA
- C.S. LA GARENA
- C.S. LUIS VIVES
- C.S. MANUEL MERINO
- C.S. MARÍA DE GUZMÁN
- C.S. MIGUEL DE CERVANTES
- C.S. NUESTRA SRA. DEL PILAR
- C.S. PUERTA DE MADRID
- C.S. REYES MAGOS

MADRID
- C.S. ALAMEDA DE OSUNA
- C.S. ALPES
- C.S. AQUITANIA
- C.S. AVDA ARAGÓN
- C.S. BARAJAS
- C.S. BENITA DE ÁVILA
- C.S. CANAL DE PANAMÁ
- C.S. CANILLEJAS
- C.S. DOCTOR CIRAJAS
- C.S. ESTRECHO DE COREA
- C.S. GANDHI
- C.S. GARCÍA NOBLEJAS
- C.S. JAZMÍN
- C.S. MAR BÁLTICO
- C.S. MONÓVAR
- C.S. REJAS
- C.S. SANCHINARRO
- C.S. SILVANO
- C.S. VICENTE MUZAS
- C.S.VIRGEN DEL CORTIJO

MECO
- C.S. MECO
  - C.L. CAMARMA DE ESTERUELAS
  - C.L. LOS SANTOS DE LA HUMOSA
  - C.L. VALDEAVERO

TORREJÓN DE ARDOZ
- C.S. BRÚJULA
- C.S. EL JUNCAL
- C.S. LA PLATA
- C.S. LA VEREDILLA
- C.S. LAS FRONTERAS
- C.S. LOS FRESNOS

TORRES DE LA ALAMEDA
- C.S. TORRES DE LA ALAMEDA
  - C.L. ANCHUELO
  - C.L. CORPA
  - C.L. LOS HUEROS
  - C.L. PEZUELA DE LAS TORRES
  - C. L. SANTORCAZ
  - C.L. VALVERDE DE ALCALÁ
  - C.L. VILLALBILLA
  - C. L. ZULEMA

Dirección asistencial Sureste

ARGANDA
- C.S. ARGANDA DEL REY
- C.S. ARGANDA-FELICIDAD
  - C.L. LA POVEDA

CAMPO REAL
- C.S. CAMPO REAL
  - C.L. LOECHES
  - C.L. POZUELO DEL REY
  - C.L. AMBITE
  - C.L. NUEVO BAZTÁN
  - C.L. OLMEDA DE LAS FUENTES
  - C.L. VILLAR DEL OLMO

COSLADA
- C.S. CIUDAD SAN PABLO
- C.S. DR. TAMAMES
- C.S. EL PUERTO
- C.S. JAIME VERA
- C.S. VALLEAGUADO
  - C.L. LA ESTACIÓN

MADRID
- C.S. ADELFAS
- C.S. ALCALÁ DE GUADAIRA
- C.S. ANGELA URIARTE
- C.S. ARROYO MEDIA LEGUA
- C.S. ARTILLEROS
- C.S. BUENOS AIRES
- C.S. CAMPO DE LA PALOMA
- C.S. CERRO ALMODOVAR
- C.S. ENSANCHE VALLECAS
- C.S. ENTREVÍAS
- C.S. FEDERICA MONTSENY
- C.S. IBIZA
- C.S. JOSÉ MARIA LLANOS
- C.S. MARTINEZ DE LA RIVA
- C.S. NUMANCIA
- C.S. PACÍFICO
- C.S. PAVONES
- C.S. PEÑA PRIETA
- C.S. RAFAEL ALBERTI
- C.S. TORITO
- C.S. VALDEBERNARDO
- C.S. VICENTE SOLDEVILLA
- C.S. VILLA VALLECAS
- C.S. VILLABLANCA

MEJORADA DEL CAMPO
- C.S. MEJORADA DEL CAMPO
  - C.L. VELILLA DE SAN ANTONIO

PERALES DE TAJUÑA
- C.S. PERALES DE TAJUÑA
  - C.L. CARABAÑA
  - C.L. MORATA DE TAJUÑA
  - C.L. ORUSCO DE TAJUÑA
  - C.L. TIELMES
  - C.L. VALDILECHA

RIVAS
- C.S. LA PAZ
- C.S. SANTA MÓNICA
- C.S. 1º DE MAYO

SAN FERNANDO DE HENARES
- C.S. SAN FERNANDO I
- C.S. SAN FERNANDO II (LOS ALPERCHINES)

VILLAREJO DE SALVANÉS
- C.S. VILLAREJO DE SALVANÉS
  - C.L. ALDARACETE
  - C.L. BELMONTE DEL TAJO
  - C.L. BREA DEL TAJO
  - C.L. ESTREMERA
  - C.L. FUENTIDUEÑA DEL TAJO
  - C.L. VILLAMANRIQUE DE TAJO

2

Dirección asistencial Sur	Dirección asistencial Oeste
ARANJUEZ C.S. ARANJUEZ C.S. LAS OLIVAS CIEMPOZUELOS C.S. CIEMPOZUELOS C.L. TITULCIA COLMENAR DE OREJA C.S. COLMENAR DE OREJA C.L. CHINCHÓN C.L. VALDELAGUNA C.L. VILLACONEJOS GETAFE C.S. BERCIAL C.S. CIUDADES C.S. EL GRECO C.S. GETAFE NORTE C.S. JUAN DE LA CIERVA C.S. MARGARITAS C.S. SECTOR III C.S. SÁNCHEZ MORATE GRIÑÓN C.S. GRIÑÓN C.L. BATRES C.L. CASARRUBUELOS C.L. CUBAS DE LA SAGRA C.L. SERRANILLOS DEL VALLE C.L. TORREJÓN DE LA CALZADA C.L. TORREJÓN DE VELASCO LEGANÉS C.S. HUERTA DE LOS FRAILES C.S. JAIME VERA C.S. LEGANES NORTE C.S. MARIA ÁNGELES LÓPEZ GÓMEZ C.S. MARIA JESUS HEREZA-CUELLAR C.S. MARIA MONTESSORI C.S. MARIE CURIE C.S. MENDIGUCHIA CARRICHE C.S. SANTA ISABEL PARLA C.S. ISABEL II C.S. LAS AMERICAS C.S. LOS PINTORES C.S. SAN BLAS C.S. PARQUE EUROPA C.S. PINTO SAN MARTÍN DE LA VEGA C.S. SAN MARTÍN DE LA VEGA VALDEMORO C.S. EL RESTÓN C.S. VALDEMORO	ALCORCÓN C.S. DR. TRUETA C.S. GREGORIO MARAÑÓN C.S. LA RIVOTA C.S. LOS CASTILLOS C.S. MIGUEL SERVET C.S. PEDRO LAIN ENTRALGO C.S. RAMÓN Y CAJAL CADALSO DE LOS VIDRIOS C.S. CADALSO DE LOS VIDRIOS C.L. CENICIENTOS C.L. ROZAS DE PUERTO REAL FUENLABRADA C.S. ALICANTE C.S. CASTILLA LA NUEVA C.S. CUZCO C.S. EL NARANJO C.S. FRANCIA C.S. PANADERAS C.S. PARQUE LORANCA C.L. PARQUE DE MIRAFLORES HUMANES DE MADRID C.S. HUMANES DE MADRID C.S. CAMPOHERMOSO C.L. MORALEJA DE ENMEDIO MOSTOLES C.S. ALCALDE BARTOLOMÉ GONZÁLEZ C.S. BARCELONA C.S. DOS DE MAYO C.S. DR. LUENGO RODRIGUEZ C.S. EL SOTO C.S. FELIPE II C.S. LA PRINCESA C.S. PARQUE COIMBRA C.L. ARROYOMOLINOS C.S. PRESENTACIÓN SABIO NAVALCARNERO C.S. NAVALCARNERO C.L. EL ALAMO C.L. SEVILLA LA NUEVA C.L. VILLAMANTA C.L. VILLAMANTILLA C.L. VILLANUEVA DE PERALES NAVAS DEL REY C.S. NAVAS DEL REY C.L. CHAPINERIA C.L. COLMENAR DE ARROYO SAN MARTÍN DE VALDEIGLESIAS C.S. SAN MARTIN DE VALDEIGLESIAS C.L. PELAYOS DE LA PRESA VILLA DEL PRADO C.S. VILLA DEL PRADO C.L. ALDEA DEL FRESNO VILLAVICIOSA DE ODÓN C.S. VILLAVICIOSA DE ODÓN

3

Dirección asistencial Noroeste	Dirección asistencial Centro
BOADILLA DEL MONTE C.S. CONDES DE BARCELONA C.S. INFANTE D. LUIS CERCEDILLA C.S. CERCEDILLA C.L. NAVACERRADA C.L. LOS MOLINOS COLLADO-VILLALBA C.S. COLLADO-VILLALBA ESTACIÓN C. L. ALPEDRETE C.S. COLLADO-VILLALBA PUEBLO C.L. MORALZARZAL C.S. SIERRA DE GUADARRAMA GALAPAGAR C.S. GALAPAGAR C.L. COLMENAREJO GUADARRAMA C.S. GUADARRAMA C.L. BECERRIL DE LA SIERRA C.L. COLLADO MEDIANO LAS ROZAS C.S. LAS ROZAS C.S. MONTERROZAS C.L. LAS MATAS MADRID C.S. ALAMEDA C.S. ARAVACA C.S. ARGÜELLES C.S. CÁCERES C.S. CASA DE CAMPO C.S. CORTES C.S. DELICIAS C.S. EL PARDO C.L. MINGORRUBIO C.S. EMBAJADORES C.S. ISLA DE OZA C.S. JUSTICIA C.S. LAVAPIÉS C.S. LEGAZPI C.S. LINNEO C.S. Mª AUXILIADORA C.S. MARTÍN DE VARGAS C.S. PALMA NORTE C.S. PÁRROCO JULIO MORATE C.S. PASEO IMPERIAL C.L. ANTONIO LEYVA C.S. SEGOVIA C.S. VALDEZARZA-SUR C.S. VENTURA RODRÍGUEZ MAJADAHONDA C.S. CERRO DEL AIRE C.S. VALLE DE LA OLIVA POZUELO DE ALARCÓN C.S. POZUELO ESTACIÓN C.S. SAN JUAN DE LA CRUZ C.S. SOMOSAGUAS ROBLEDO DE CHAVELA C.S. ROBLEDO DE CHAVELA C.L. FRESNEDILLAS DE LA OLIVA C.L. NAVALAGAMELLA C.L. NAVALESPINO C.L. ROBLEDONDO C.L. S. M. DE LA ALAMEDA ESTACIÓN C.L. S.M. DE LA ALAMEDA PUEBLO C.L. VALDEMAQUEDA C.L. ZARZALEJO ESTACIÓN C.L. ZARZALEJO PUEBLO SAN LORENZO DEL ESCORIAL C.S. SAN CARLOS C.L. EL ESCORIAL C.L. LOS ARROYOS C.L. VALDEMORILLO TORRELODONES C.S. TORRELODONES C.L. HOYO DE MANZANARES VILLANUEVA DE LA CAÑADA C.S. VILLANUEVA DE LA CAÑADA C.L. BRUNETE C.L. QUIJORNA C.L. VILLAFRANCA DEL CASTILLO C.L. VILLANUEVA DEL PARDILLO	MADRID C.S. ABRANTES C.S. ALMENDRALES C.S. ANDRÉS MELLADO C.S. BAVIERA C.S. CAMPAMENTO C.S. CARABANCHEL ALTO C.S. CARAMUEL C.S. CASTELLÓ C.S. CEA BERMÚDEZ C.S. CIUDAD JARDÍN C.S. COMILLAS C.S. DAROCA C.S. EL ESPINILLO C.S. ELOY GONZALO C.S. ESPRONCEDA C.S. GENERAL FANJUL C.S. GENERAL RICARDOS C.S. GOYA C.S. GUAYABA C.S. GUZMÁN EL BUENO C.S. JOAQUÍN RODRIGO C.S. LAGASCA C.S. LAS ÁGUILAS C.S. LAS CALESAS C.S. LONDRES C.S. LOS ÁNGELES C.S. LOS CÁRMENES C.S. LOS ROSALES C.S. LOS YÉBENES C.S. LUCERO C.S. MAQUEDA C.S. MONTESA C.S. NUESTRA SRA. DE FÁTIMA C.S. ORCASITAS C.S. ORCASUR C.S. PERALES DEL RÍO C.S. POTES C.S. POTOSÍ C.S. PRÍNCIPE DE VERGARA C.S. PROSPERIDAD C.S. PUERTA BONITA C.S. PUERTA DEL ÁNGEL C.S. QUINCE DE MAYO C.S. SAN ANDRÉS C.S. SAN CRISTÓBAL C.S. SAN FERMÍN C.S. SANTA HORTENSIA C.S. SEGRE C.S. VALLE INCLÁN

Anexo [NN] Listado de hospitales de la red del Servicio Madrileño de Salud, de la web de la Consejería de Sanidad de la Comunidad de Madrid. Con los datos de cada uno de los hospitales que aparece en el Catálogo Nacional de hospitales de 2018, del Ministerio de Sanidad, Consumo y Bienestar social. Fecha 31/05/2021.

	Tipo	Nombre de Hospital o Complejo (1)	Camas	Finalidad	Dependencia funcional	Dependencia Patrimonial	Concierto	Acreditación docente
1	Hospital	Hospital General Universitario Gregorio Marañón	1.351	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
2	Hospital	Hospital Universitario 12 de Octubre	1.256	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
3	Complejo	Hospital Universitario La Paz Hospital Carlos III Hospital Cantoblanco	1.254	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
4	Hospital	Hospital Universitario Ramón y Cajal	891	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
5	Hospital	Hospital Clínico San Carlos	860	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
6	Hospital	Hospital Universitario Puerta de Hierro Majadahonda	613	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
7	Hospital	Hospital Universitario de La Princesa	564	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	N
8	Hospital	Hospital Universitario de Getafe	510	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	N
9	Hospital	Hospital Universitario Príncipe de Asturias	507	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
10	Hospital	Hospital Universitario de Fuenlabrada	406	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
11	Hospital	Hospital Universitario Fundación Alcorcón	400	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
12	Hospital	Hospital Universitario Severo Ochoa	386	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
13	Complejo	Hospital Universitario Infanta Leonor Hospital Virgen de la Torre	367	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	N
14	Hospital	Hospital Universitario Rey Juan Carlos	364	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
15	Hospital	Hospital Universitario de Móstoles	332	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
16	Hospital	Hospital Universitario Infanta Sofía	271	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
17	Hospital	Hospital Universitario de Torrejón	250	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
18	Hospital	Hospital Universitario del Henares	238	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
19	Hospital	Hospital General de Villalba	209	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
20	Hospital	Hospital Virgen de la Poveda	202	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
21	Hospital	Hospital Universitario Infanta Cristina	188	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
22	Hospital	Hospital Universitario Santa Cristina	156	GENERAL	SERMAS	SEGURIDAD SOCIAL	N	S
23	Hospital	Hospital Central de la Cruz Roja San José y Santa Adela	154	GENERAL	SERMAS	PRIVADO/BENEFICO	N	S
24	Hospital	Hospital Universitario Infanta Elena	152	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	N
25	Hospital	Hospital Universitario del Sureste	132	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
26	Hospital	Hospital Universitario del Tajo	98	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	S
27	Hospital	Hospital El Escorial	91	GENERAL	SERMAS	COMUNIDAD AUTONOMA	N	N
28	Hospital	Hospital La Fuenfría	192	GERIATRIA	SERMAS	SEGURIDAD SOCIAL	N	S
29	Hospital	Hospital de Guadarrama	144	GERIATRIA	SERMAS	COMUNIDAD AUTONOMA	N	S
30	Hospital	Hospital Infantil Universitario Niño Jesús	174	INFANTIL	SERMAS	COMUNIDAD AUTONOMA	N	N
31	Hospital	Hospital Dr. Rodríguez Lafora	334	PSIQUIATRICO	SERMAS	COMUNIDAD AUTONOMA	N	S
32	Hospital	Instituto Psiquiátrico Servicios de Salud Mental José Germain	178	PSIQUIATRICO	SERMAS	COMUNIDAD AUTONOMA	N	S
32	Hospital	Hospital Fundación Jiménez Díaz	659	GENERAL	PRIVADO	PRIVADO / NO BENEFICO	S	S
33	Hospital	Hospital Central de la Defensa "Gómez Ulla"	475	GENERAL	Min. de Defensa	Min. de Defensa	S	S
		Suma	**14.358**					

Fuente datos columnas: Catálogo Nacional de Hospitales 2018. Min. de Sanidad, Consumo y Bienestar Social. https://www.mscbs.gob.es/ciudadanos/prestaciones/centrosServiciosSNS/hospitales/docs/2018_CNH.pdf
(1) El listado suministrado por la Comunidad Autonoma de Madrid.Web: Hospitales de la red del Servicio Madrileño de Salud https://www.comunidad.madrid/servicios/salud/hospitales-red-servicio-madrileno-salud

mayo 2020