Universidad CEU San Pablo
CEINDO – CEU Escuela Internacional de Doctorado

PROGRAMA EN DERECHO Y ECONOMÍA

La protección de datos personales en el ámbito de la salud: transparencia y acceso a la información pública sanitarias

TESIS DOCTORAL

Presentada por:
Julia Merino Martín

Dirigida por:
José Luis Piñar Mañas
Alejandro Corral Sastre

MADRID
2020

DEDICATORIA Y AGRADECIMIENTOS

Dedico esta tesis a mi familia. A mi madre por ser estimulo constante en mi vida y a la que tanto debo.

A mis hijos, por su apoyo incondicional y ser fuente de mi motivación e inspiración para superarme cada día más.

A mi marido porque sin su comprensión, sacrificio y ánimo no hubiera sido posible mi dedicación a esta tesis.

Dedico también esta tesis y mi más profunda gratitud y reconocimiento a mis directores José Luis Piñar Mañas y Alejandro Corral Sastre, suyo es el impulso en este trabajo. Su motivación permanente, no me dejo desfallecer en este esfuerzo. Su rigor en la dirección y supervisión han sido clave en el resultado, al que he intentado responder con esfuerzo, dedicación y el espíritu de trabajo que me han guiado para plasmar el saber científico en esta tesis. El trato personal que me han dispensado a lo largo de estos años, se merece el mayor de mis respetos y el gran aprecio que siento por ellos.

Finalmente va dedicado a mis compañeros y amigos, presentes y pasados, y a todas aquellas personas que durante estos años estuvieron a mi lado apoyándome.

"El Reglamento Europeo de Protección de Datos introduce, a veces directamente, a veces de forma algo soterrada, un nuevo modelo de protección de datos para Europa. Un nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información".

José Luis Piñar Mañas

ÍNDICE

ABREVIATURAS 15

INTRODUCCIÓN 17

I. ACOTACIÓN Y DELIMITACIÓN TEMÁTICA 17

II. OBJETIVOS Y JUSTIFICACIÓN 22

III. ESTRUCTURA Y METODOLOGÍA 24

PARTE I. LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA SALUD

CAPÍTULO I. EL DERECHO A LA PROTECCIÓN DE DATOS

1. EL DERECHO A LA PROTECCIÓN DE DATOS 33

1.1. EL DERECHO A LA INTIMIDAD COMO OBJETO DE LA PROTECCIÓN DE DATOS 33

1.1.1. ÁMBITO CONSTITUCIONAL: DELIMITACIÓN DE SU CONTENIDO ESENCIAL 33

1.1.2. LA PROTECCIÓN DE DATOS COMO DERECHO AUTÓNOMO FRENTE A LA INTIMIDAD 37

1.1.2.1. **Diferencias entre ambos derechos** 39

1.2. RECONOCIMIENTO DEL DERECHO A LA PROTECCIÓN DE DATOS 42

1.2.1. PRECEDENTES NORMATIVOS Y JURISPRUDENCIALES INTERNACIONALES EUROPEOS 42

1.2.1.1. **Convenio 108 y Directiva 95/46 CE** 47

1.2.1.1.1. **Convenio 108** 48

1.2.1.2. **Principios relativos al tratamiento de datos personales, recogidos en la normativa del Consejo de Europa (Resoluciones y Convenio 108)** 50

1.2.1.3. **Unión Europea** 52

1.2.1.4. **Directiva sobre protección de datos en el ámbito penal** 55

1.2.1.5. **Directiva sobre la privacidad y las comunicaciones electrónicas** 56

1.2.1.6. **Reglamento relativo al tratamiento de los datos personales de las instituciones y los organismos de la Unión** 56

1.2.1.7. **Otra normativa europea** 56

1.2.1.8. **La protección de datos en la normativa y actos sectoriales** 57

1.2.2. LA LIBERTAD INFORMÁTICA Y EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA 58

1.2.2.1. **Reconocimiento constitucional** 60

1.2.3. RECONOCIMIENTO DEL DERECHO A LA PROTECCIÓN DE DATOS: DOCTRINA CONSTITUCIONAL 63

1.2.3.1. **Doctrina constitucional** 70
1.2.3.2. **Reconocimiento legal** 75

2 GARANTÍAS DEL SISTEMA 77

2.1. AUTORIDADES DE CONTROL 77

2.1.1. NECESIDAD Y TRASCENDENCIA DE LAS GARANTÍAS FRENTE A LA INVASIÓN DE LA PRIVACIDAD 77

2.1.1.1. **Medidas provisionales de garantía de los derechos en materia de protección de datos** 79

2.1.2. AUTORIDADES DE CONTROL INDEPENDIENTES 82

2.1.2.1. **Independencia** 85

2.1.3. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (SUEPD) 89

2.1.4. AUTORIDADES NACIONALES Y AUTONÓMICAS 90

2.1.4.1. **La Agencia Española de Protección de Datos** 90
2.1.4.2. **Autoridades autonómicas de control** 92

2.2. SISTEMA SANCIONADOR 93

2.2.1. INFRACCIONES Y SANCIONES 93

2.2.2. PROCEDIMIENTO SANCIONADOR 102

CAPÍTULO II. DATOS PERSONALES EN EL ÁMBITO DE LA SALUD

1. CATEGORÍAS ESPECIALES DE DATOS PERSONALES 107

1.1. DATOS SENSIBLES ESPECIALMENTE PROTEGIDOS 107

1.2. DATOS RELATIVOS A LA SALUD 110

1.2.1. ELEMENTOS CONSTITUTIVOS 110

1.2.2. LOS DATOS DE SALUD EN EL RGPD, EN LA LOPDGDD Y EN LA NORMATIVA SECTORIAL DE SALUD: NUEVAS CATEGORÍAS DE DATOS SENSIBLES 114

1.2.3. DERECHOS DE LOS PACIENTES A LA CONFIDENCIALIDAD DE SUS DATOS Y OBLIGADO SECRETO DE LOS PROFESIONALES 118

1.2.4. DOCUMENTACIÓN CLÍNICO-SANITARIA PORTADORA DE DATOS DE SALUD ... 123

1.2.4.1. **Documento de voluntades anticipadas** 124
1.2.4.2. **Recetas médicas y Órdenes de dispensación: sus implicaciones en materia de protección de datos** 126
1.2.4.3. **Receta electrónica** 127

1.3. PROTECCIÓN DE DATOS EN LA INVESTIGACIÓN BIOMÉDICA 129
1.3.1. PROTECCIÓN DE LA INTIMIDAD EN LOS PROYECTOS DE INVESTIGACIÓN 129
1.3.2. MEDIDAS PARA EVITAR LA IDENTIFICACIÓN DEL INTERESADO 131

2. TRATAMIENTO Y CESIÓN DE DATOS DE SALUD 133
2.1. PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS DE SALUD 133
2.1.1. PRINCIPIO DE CALIDAD DE LOS DATOS 136
2.1.2. PRINCIPIO DE TRANSPARENCIA 142
2.1.3. PRINCIPIO DE CONSENTIMIENTO 145
2.1.4. PRINCIPIOS CONTENIDOS EN EL RGPD Y EN LA LOPDGDD 148
2.1.4.1. **Principio de licitud, lealtad y transparencia** 149
2.1.4.2. **Principio de limitación de finalidad** 150
2.1.4.3. **Principio de minimización de datos** 151
2.1.4.4. **Principio de exactitud y veracidad** 152
2.1.4.5. **Principio de limitación del plazo de conservación** 153
2.1.4.6. **Principio de integridad y seguridad** 154
2.2. DERECHOS DE LOS TITULARES DE LOS DATOS 154
2.2.1. OTRA CLASIFICACIÓN, DISTINTA DE LOS DERECHOS ARCO 154
2.2.1.1. **Derecho de rectificación** 159
2.2.1.2. **Derecho de cancelación** 161
2.2.1.3. **Derecho de limitación del tratamiento** 162
2.2.1.4. **Derecho de oposición y decisiones individuales automatizadas** 164
2.2.1.4.1. ***Decisiones individuales automatizadas*** 165
2.2.1.5. **Derecho a la supresión o al olvido** 167
2.2.1.5.1. ***Supresión de datos en la Historia Clínica*** 175
2.2.1.6. **Derecho a la portabilidad de los datos** 176
2.2.1.7. **Los nuevos Derechos Digitales que pueden afectar a los datos de salud** 179
2.2.2. EJERCICIO DE LOS DERECHOS DEL PACIENTE FRENTE AL TRATAMIENTO DE DATOS DE SALUD 183
2.2.2.1. **La Historia Clínica : HC digital** 183
***i) Contenido y* finalidad** 183
ii) La Historia Clínica como portador esencial de datos sanitarios 185
***iii) Historia Clínica Digital): problemática en cuanto a la protección de* datos** 186
2.2.2.2. **Acceso a los datos de salud** 190
i) Derecho de acceso. Conflicto entre accesibilidad y protección de la Historia Clínica 192
ii) Acceso de pacientes/usuarios a su Historia Clínica 194
iii) Acceso a la Historia Clínica por profesionales sanitarios con fines asistenciales 196
iv) Acceso por terceros a la Historia Clínica 197

v) Acceso a la Historia Clínica de personas fallecidas 205

2.3. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS DE SALUD 207

2.3.1. TRATAMIENTO DE DATOS PERSONALES 207

2.3.1.1. **Consideraciones previas** 207
2.3.1.2. **Licitud del tratamiento** 209
2.3.1.3. **Responsable-Encargado del tratamiento** 210

2.3.2. CONSENTIMIENTO Y OTRAS BASES LEGITIMADORAS DEL TRATAMIENTO DE DATOS DE SALUD 215
2.3.2.1. **Requisitos del consentimiento** 216
2.3.2.1.1. ***Especificidades del consentimiento para el tratamiento de datos de salud*** 222
2.3.2.1.2. ***En cuanto a la forma de prestar el consentimiento*** 224
2.3.2.2. **Condicionantes de la licitud del consentimiento** 225
2.3.2.3. **Otras bases legitimidadoras del tratamiento de datos de salud: el interés público** 228
2.3.2.3.1. ***El interés público como base legitimadora de los datos de salud*** 233

3. ANÁLISIS CRÍTICO DE ALGUNOS TRATAMIENTOS DE DATOS DE SALUD 238

3.1. SITUACIONES DE URGENCIA VITAL 238

3.2. UTILIZACIÓN DE DATOS DE SALUD POR COMPAÑÍAS ASEGURADORAS 242

3.3. ACCESO A DATOS DE SALUD POR SERVICIOS EXTERNALIZADOS 244

4. SEGURIDAD DE LOS DATOS SANITARIOS 246

4.1. RIESGOS EN LA PROTECCIÓN DE DATOS SANITARIOS 247

4.2. SUPERVISIÓN DEL TRATAMIENTO DE DATOS DE SALUD: DELEGADO DE PROTECCIÓN DE DATOS 248

4.3. MEDIDAS DE SEGURIDAD Y VIOLACIÓN DE LA SEGURIDAD EN EL ÁMBITO SANITARIO 250

4.3.1. MEDIDAS DE SEGURIDAD A ADOPTAR POR LAS ENTIDADES PÚBLICAS 255

4.4. RESPONSABILIDAD PROACTIVA EN EL TRATAMIENTO DE DATOS DE SALUD 257

4.5. SEUDONIMIZACIÓN Y ANONIMIZACIÓN COMO TÉCNICAS DE SEGURIDAD DE LOS DATOS SANITARIOS 263

5. PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA ASISTENCIA SANITARIA TRANSFRONTERIZA 267

5.1. TRANSFERENCIAS INTERNACIONALES DE DATOS 267

5.2. PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA ASISTENCIA SANITARIA TRANSFRONTERIZA 276

5.2.1. ASISTENCIA SANITARIA Y PROTECCIÓN DE DATOS 276

5.2.2. INTEROPERABILIDAD DE LOS SISTEMAS SANITARIOS 280

PARTE II. LA PROTECCIÓN DE DATOS Y LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA SANITARIAS

CAPÍTULO I. TRANSPARENCIA EN LA ACTIVIDAD PÚBLICA SANITARIA

1. LA TRANSPARENCIA COMO ELEMENTO ESENCIAL DE PARTICIPACIÓN Y ACCESO A LA INFORMACIÓN PÚBLICA 287

1.1. LA TRANSPARENCIA PÚBLICA 287

1.1.1. NORMATIVA REGULADORA DE LA TRANSPARENCIA PÚBLICA 295

1.2. TRANSPARENCIA DE LA ACTIVIDAD PÚBLICA SANITARIA 296

2. PUBLICIDAD ACTIVA DE CONTENIDO SANITARIO 299

2.1. SUJETOS OBLIGADOS Y CARACTERÍSTICAS DE LA INFORMACIÓN 301

2.1.1. CARACTERÍSTICAS DE LA INFORMACIÓN 302

2.2. TIPOLOGÍA Y LÍMITES DE LA INFORMACIÓN 302

2.2.1. TIPOS DE INFORMACIÓN 302

2.2.2. LÍMITES DE LA INFORMACIÓN 305

2.3. PORTAL DE TRANSPARENCIA. PORTAL SANITARIO 305

2.3.1. PORTAL SANITARIO 307

CAPÍTULO II. DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA SANITARIA Y SU REUTILIZACIÓN COMO BASES DEL GOBIERNO ABIERTO

1. DERECHO DE ACCESO A LA INFORMACIÓN 311

1.1. NATURALEZA 314

1.2. LA INFORMACIÓN PÚBLICA COMO CONTENIDO DEL DERECHO DE ACCESO 319

1.2.1. DERECHO A RECIBIR INFORMACIÓN 319

1.2.2. ALCANCE DEL TÉRMINO “INFORMACIÓN PÚBLICA” 322

1.2.3. APLICACIÓN SUPLETORIA DE LA LEY DE TRANSPARENCIA Y BUEN GOBIERNO 324

1.3. INFORMACIÓN PÚBLICA DE CARÁCTER SANITARIO 326

1.3.1. CARACTERÍSTICAS 326

1.3.2. CLASES DE INFORMACIÓN SANITARIA 327

1.3.3. INFORMACIÓN SOBRE LISTAS DE ESPERA QUIRÚRGICA 336

1.4. EJERCICIO DEL DERECHO DE ACCESO 337

1.4.1. SOLICITUDES DE ACCESO Y PROCEDIMIENTO 337

1.4.2. CAUSAS DE INADMISIÓN 340

1.4.3. EXCEPCIONES AL DERECHO DE ACCESO: LÍMITES ESPECÍFICOS 350

1.4.3.1. **Sentencias sobre la limitación del derecho de acceso: ST del Juzgado Central de lo Contencioso nº 98/2017, de 22 de junio de 2017 y ST del Juzgado Central de lo Contencioso, de 14 de junio de 2016** 355

1.4.3.2. **Examen de las materias relacionadas en el art. 14.1 LTBG** 356

1.4.3.2.1. ***Intereses económicos y comerciales: Sentencia del Juzgado Central de lo Contencioso-Administrativo, de 3 abril 2018*** 357

1.4.3.2.2. ***Otros límites específicos sujetos al doble test de daño y ponderación de intereses*** 359

1.4.4. LIMITACIONES EN EL ÁMBITO SANITARIO 360

1.4.5. CONSEJO DE TRANSPARENCIA Y BUEN GOBIERNO 362

2. REUTILIZACIÓN DE LOS DATOS DE SALUD 366

2.1. CONDICIONES DE REUTILIZACIÓN DE LA INFORMACIÓN 366

2.2. OPEN DATA Y REUTILIZACIÓN DE DATOS DE SALUD 372

2.3. HERRAMIENTAS TECNOLOGÍCAS PARA EL TRATAMIENTO DE LA INFORMACIÓN EN EL ÁMBITO DE LA SALUD 378

2.4. REUTILIZACIÓN Y PROTECCIÓN DE DATOS PERSONALES 380

CAPÍTULO III. EL DERECHO A LA PROTECCIÓN DE DATOS Y EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA SANITARIAS

1. PRESUPUESTOS PARA LA APLICACIÓN DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS 383

1.1. RELACIONES ENTRE AMBOS DERECHOS 383

1.2. PRESUPUESTOS PARA LA APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS. CONSIDERACIONES SOBRE LOS DATOS DE SALUD 389

2. LA NORMATIVA SOBRE PROTECCIÓN DE DATOS COMO LÍMITE AL ACCESO A LA INFORMACIÓN PÚBLICA SANITARIA 392

2.1. LA PROTECCIÓN DE DATOS COMO LÍMITE. EN ESPECIAL LOS DATOS DE SALUD . 392

2.2. TIPOLOGÍA DE DATOS PERSONALES REGULADOS EN LA LGTB Y SU APLICACIÓN 393

2.2.1. CATEGORÍAS ESPECIALES DE DATOS: DATOS DE CONTENIDO SANITARIO 396

2.2.2. ACCESO A INFORMACIÓN QUE NO CONTIENE DATOS ESPECIALMENTE PROTEGIDOS 401

3. PROCESO APLICATIVO PARA RESOLVER LA SOLICITUD DE ACCESO A LA INFORMACIÓN EN EL ÁMBITO SANITARIO 404

3.1. VALORACIÓN ACERCA DE SI LA INFORMACIÓN SOLICITADA CONTIENE DATOS PERSONALES 404

3.2. ANÁLISIS ACERCA DE SI LA INFORMACIÓN CONTIENE DATOS DE SALUD 407

3.3. PONDERACIÓN PARTICULARIZADA DE INTERESES 408

3.3.1. CRITERIO DE LA PREVALENCIA DEL INTERÉS PÚBLICO 408

3.3.2. APLICACIÓN DE LA PONDERACIÓN DE INTERESES EN JUEGO: EXCLUSIÓN DE LOS DATOS SANITARIOS 412

3.4. PROCESO PARA RESOLVER LAS SOLICITUDES DE ACCESO 425

CONCLUSIONES 429

JURISPRUDENCIA 449

AUTORIDADES DE CONTROL 455

GT ARTÍCULO 29 459

BIBLIOGRAFÍA 461

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos.
CCAA	Comunidades Autónomas.
CE	Constitución española.
CDFUE	Carta Fundamental de los Derechos de la Unión Europea.
CEDH	Convenio para la protección de los derechos humanos y las libertades fundamentales.
Convenio 108	Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
CTBG	Consejo de Transparencia y Buen Gobierno.
Directiva 95/46/CE	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.
DPD	Delegado de Protección de Datos.
GT29	Grupo de trabajo del artículo 29 de la Directiva 95/46/CE.
HC	Historia Clínica.
LBAP	Ley Básica de Autonomía del Paciente.
LGS	Ley General de Sanidad.
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal.
LOPDGDD	Ley Orgánica de Protección de Datos personales y garantía de los derechos digitales.
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personal.

LPAC	Ley de Procedimiento Administrativo Común de las Administraciones Públicas.
LRJSP	Ley de Régimen Jurídico del Sector Público.
LTBG	Ley de Transparencia y Buen Gobierno.
RGPD	Reglamento General de Protección de Datos.
RLOPD	Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.
SAN	Sentencia de la Audiencia Nacional
SAP	Sentencia de la Audiencia Provincial
SNS	Sistema Nacional de Salud.
SPED	Supervisor Europeo de Protección de Datos.
STC	Sentencia del Tribunal Constitucional.
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos.
STPI	Sentencia del Tribunal Penal internacional.
STS	Sentencia del Tribunal Supremo.
TC	Tribunal Constitucional.
TEDH	Tribunal Europeo de Derechos Humanos.
TFUE	Tratado de Funcionamiento de la Unión Europea.
TJCE	Tribunal de Justicia de la Comunidad Europea.
TJUE	Tribunal de Justicia de la Unión Europea.
TS	Tribunal Supremo.
TUE	Tratado de la Unión Europea.

INTRODUCCIÓN

El objeto de este trabajo de investigación gira entorno al estudio de los datos personales de salud. Así, nos va a interesar analizar las peculiaridades de este tipo de datos, en la medida en que constituyen datos especialmente protegidos, afectados, además, por un componente esencial y de aplicación prioritaria y preferente como es la salud; de aplicación en los supuestos de necesaria asistencia sanitaria o protección de la salud pública. Examinaremos, por tanto, todo el amplio espectro de documentación susceptible de incluir datos personales de salud y sus manifestaciones en el terreno sanitario o de salud; determinando sus especificidades, y si confieren derechos diferenciados respecto del resto de datos de carácter personal.

I. ACOTACIÓN Y DELIMITACIÓN TEMÁTICA

En el momento de comenzar a redactar esta introducción, me ha venido la memoria la difusión de una noticia que informaba de la detención de un *Hacker* (de 16 años) por haber entrado ilegalmente en el sistema informático del Servicio Madrileño de Salud (*Horus*), y acceder (por tanto, indebidamente) a la historia clínica de un diputado muy conocido públicamente; haciéndola pública posteriormente a través de distintas redes sociales. Este pequeño flash me va a servir para comentar que la elección del tema de este trabajo haya venido por una situación personal de indignación por una amiga que fue objeto de una intromisión ilegal en su historia clínica por una trabajadora del Servicio Público de Salud, en la que participé activamente en restaurar sus derechos y su dignidad.

A este motivo de definición del objeto del trabajo, habría que añadir para reforzar, si cabe, el acaecimiento de un fenómeno que está siendo trascendental en la vida de la humanidad, como es la epidemia de COVID-19, que alcanzó su mayor virulencia en el mes de marzo 2020, coincidiendo con la declaración del Estado de Alarma (Real Decreto 463/2020, de 14 de marzo). La incidencia en la salud, economía y sociedad ha sido y está siendo (porque seguimos bajo los efectos de la pandemia) muy grande. Así, la afectación de la

salud de los ciudadanos se ha manifestado, no sólo en el número de muertes en España(se habla de más de 50.000), sino de aquellos que han sido víctimas directas o indirectas del virus; bien, contrayendo la enfermedad y asumiendo sus secuelas, bien de quienes, padeciendo patologías graves ajenas al virus, sufrieron el colapso hospitalario del

momento (marzo-abril 2020) sin poder recibir asistencia sanitaria, incrementando así el número de fallecidos directos por la epidemia.

Durante el período inicial de la pandemia (y que se mantiene, aunque a menor nivel) la anormalidad alcanzó no sólo a la economía y a la sociedad, sino que afectó a la propia educación o enseñanza, en todas sus etapas y grados; llegando por tanto a los doctorados. Sin perjuicio de señalar estos efectos prevalentes, también existe una afectación personal, de menor alcance, por supuesto, como consecuencia de los efectos tantos duros de la epidemia (situación que sigue al continuar la pandemia), y que han tenido su efecto sobre el desarrollo normal de este trabajo de investigación: primero, en las fechas de entrega del mismo y, segundo, obligándome a una indeseada e improvisada ejecución del trabajo consecuencia de lo extraordinario de los acontecimientos del momento.

Ya que, como indicamos, la situación de epidemia continúa, ha sido necesario volver adoptar medidas específicas de actuación por razón de salud pública. Así, por parte del Estado, se dictó el Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19, en cuyo art. 27 se establecía que el tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y aplicación del citado Real Decreto-ley se hará de acuerdo a lo dispuesto en el RGPD, en la LOPDGDD, y en lo establecido en los artículos ocho.1 y veintitrés de la LGS. Señalando, asimismo, que las obligaciones de información a los interesados relativas a los datos obtenidos por los sujetos incluidos en el ámbito de aplicación del presente Real Decreto-ley se ajustarán a lo dispuesto en el artículo 14 RGPD, teniendo en cuenta las excepciones y obligaciones previstas en su apartado 5.

Por otra parte, la finalidad del tratamiento de esta información será el seguimiento y vigilancia epidemiológica del COVID-19 para prevenir y evitar situaciones excepcionales de especial gravedad, atendiendo a razones de interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y

de otras personas físicas al amparo de lo establecido en RGPD. Concluyendo que los datos recabados serán utilizados exclusivamente con esta finalidad.

Conforme ha ido evolucionando la pandemia, los distintos gobiernos autonómicos (en función de la entidad de la situación) han ido adoptando medidas formalizadas mediante distintos instrumentos legales. Así, la Comunidad de Madrid dicto la Orden 1262/2020, de 30 de septiembre, de la Consejería de Sanidad, dirigida a asegurar el control del cumplimiento de las obligaciones de aislamiento para la contención del virus. De esta norma, a efectos de este trabajo, nos interesa destacar su fundamentación jurídica:

Por ello, de una parte, la Ley Orgánica 3/1986, de 14 de abril, en su art. 2 faculta a las autoridades sanitarias competentes para adoptar medidas de reconocimiento, tratamiento, hospitalización o control cuando se aprecien indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas, o por las condiciones sanitarias en las que se desarrolle una actividad. A su vez, el artículo 3 de dicha Ley Orgánica señala que, con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las oportunas medidas para el control de los enfermos, de las personas que estén o hayan estado en contacto y del medio ambiente inmediato, así como las que se consideren precisas en caso de riesgo de carácter transmisible.

Por su parte, la Ley 14/1986, de 14 de abril, General de Sanidad, en su art. 26, dispone que en el caso de que exista o se sospeche razonablemente la existencia de un riesgo inminente y extraordinario para la salud, las autoridades sanitarias adoptarán las medidas preventivas que estimen oportunas, como por ejemplo la intervención de medios materiales y personales, y todas las que se consideren sanitariamente justificadas.

Asimismo, la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud, establece en su artículo 65, la posibilidad de adoptar actuaciones coordinadas en materia de salud pública, para responder a situaciones de especial riesgo o alarma para la salud pública.

La Ley 33/2011, de 4 de octubre, General de Salud Pública, establece, en su art. 54, que con carácter excepcional y cuando así lo requieran motivos de extraordinaria gravedad o

urgencia, la posibilidad de adoptar medidas adicionales en caso de riesgo de transmisión de enfermedades.

Referido, más en concreto al tratamiento de datos de salud, el art. 16.3 LBAP, relativo a los usos de la historia clínica, determina que el acceso a la misma con fines epidemiológicos o de salud pública se regirá por la legislación vigente en materia de protección de datos personales y la Ley 14/1986, de 25 de abril, General de Sanidad, y resto de normas de aplicación en cada caso; concretando que, cuando sea preciso para la prevención de un riesgo o grave peligro para la salud de la población, las administraciones sanitarias a las que se refiere el artículo 41 de la Ley 33/2011, de 4 de octubre, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública y que su acceso determina una obligación equivalente a la de secreto.

Señala la indicada orden, tomando como fuente el RGPD, que éste "*contiene salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones como la actual, en la que existe una emergencia sanitaria de alcance generalizado, por lo que, en aplicación de los preceptos previstos en el RGPD, en consonancia con la normativa sectorial aplicable en el ámbito de la salud pública, las consideraciones relacionadas con la protección de los datos de carácter personal —dentro de las limitaciones previstas en las leyes— no deberían utilizarse para obstaculizar o limitar la efectividad de las medidas adoptadas por la autoridad sanitaria en la lucha contra la epidemia, dado que dicha normativa de protección de datos contiene una regulación para estas situaciones que compatibiliza y pondera los intereses y derechos afectados para asegurar el bien común y el interés público*".

Del mismo modo, apoyándose en el Considerando 46 del Reglamento viene a reconocer 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 o el de otras personas físicas: 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 en base al 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 sea necesario para fines sanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia sanitaria, sobre todo caso de catástrofes naturales o de origen humano".

Como excepciones a la prohibición general de tratamiento de los datos de salud (y, por tanto de los especialmente protegidos), el propio Reglamento lo excepciona en base a las habilitaciones contenidas en el art. 9: en base a razones de interés público esencial, debiendo ser proporcional al objetivo perseguido y respetar la esencia del derecho a la protección de datos (apartado.2.g); que el tratamiento es necesario a los fines previstos en el apartado.2.h), como fines de medicina preventiva o laboral de los trabajadores, o gestión de los sistemas de asistencia sanitaria, entre otros; y si el tratamiento es necesario en el ámbito de la salud pública (apartado.2.i).

No obstante, la indicada normativa, se ha puesto de manifiesto la insuficiente cobertura legal de las denominadas "grandes" leyes sanitarias de que dispone nuestro país. Así, tanto la Ley 3/1986, de 14 de abril y la Ley 33/2011, de 4 de octubre (aún no desarrollada), en situaciones, como la presente, adolecen de suficiente concreción, presentando grandes lagunas jurídicas que dificultan su aplicación a esta situación. De ahí, que, tanto por dirigentes políticos como por operadores jurídicos se haya señalado la necesidad urgente de modificar y adaptar estas leyes; o bien, elaborar una nueva Ley de Salud que delimite las competencias entre el Estado y las CCAA, dotando de instrumentos suficientes para hacer frente a situaciones pandémicas de gran alcance como la presente.

Esta insuficiente falta de cobertura jurídica para adoptar medidas contra la pandemia que puedan afectar a derechos fundamentales se está poniendo de manifiesto con más intensidad, si cabe, en el momento de la segunda oleada del virus, en la que se anuncia que, ante la imposibilidad de que las CCAA cuente con instrumentos jurídicos válidos para adoptar medidas de confinamiento de la población, resulta necesario que éstas únicamente puedan realizarse dentro del estado de alarma, previamente declarado por el Estado. En este sentido, se ha dictado 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; el cual no prevé la posibilidad de medidas limitativas de los derechos fundamentales.

Implícita en la declaración del Estado de Alarma se incluía la regulación especial de aspectos relacionados con el objeto de este trabajo y que en su ejecución constituyeron una problemática discutible. Así, como señaló la AEPD, no hay una suspensión del derecho a la protección de datos personales, debiendo respetarse los derechos y garantías de los afectados en el tratamiento de datos, de forma que los datos a utilizar serán los exclusivamente necesarios para controlar la pandemia; sin que puedan ser un obstáculo a la asistencia sanitaria; de forma que sigan respetando los derechos y garantías de los afectados, en el tratamiento de datos, en especial, del principio de minimización de datos, de forma 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"*; como la utilización de técnicas de geolocalización a través de dispositivos móviles que puedan emitir avisos (anónimos) de afectación por el Coronavirus.

A propósito de la base legitimadora de "la salud pública", la AEPD ha emitido un comunicado como consecuencia de la epidemia del Coronavirus, señalando que esta epidemia no puede significar una suspensión del derecho fundamental a la protección de datos, y que, al mismo tiempo, su normativa reguladora no puede suponer un entorpecimiento de la asistencia sanitaria en esta situación.

II. OBJETIVOS Y JUSTIFICACIÓN

Partiendo de que los datos de salud suponen un elemento esencial para la promoción y mejora de la salud de las personas; ya que, en concreto, los datos clínicos de un paciente son el instrumento que utiliza el profesional médico para emplearlos en su proceso curativo; vamos a situar nuestro eje central en los datos sanitarios o de salud. Procedemos a analizar la problemática de este tipo de datos (especialmente protegidos) y su relación con la tipología general de datos personales; a fin de determinar si estamos o no ante una tipología de datos en la que se manifiestan especificidades que lleguen a suponer derechos diferenciados del tipo general, en la medida en que, quizás, debe ceder la observancia de

los principios y normas de la protección de datos en favor del bien superior que constituye la protección de la salud y de la vida de las personas.

Todo ello, considerando la posibilidad que atribuye al Estado el RGPD (art. 9.4) de "*mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud*".

Para una mejor fundamentación de la hipótesis vamos a partir de una realidad constatada: tratándose de datos de salud, en ocasiones, la normativa sanitaria específica regula actuaciones clínicas o sanitarias que tienen un componente de datos personales de una persona que vienen a diferir del conjunto de reglas generales establecidos por el RGPD y la LOPDGDD para el resto de datos personales. Así, esta singularidad nos va a dar pie a plantear nuestras hipótesis del trabajo, analizando; de una parte, la materia a raíz de los recientes y trascendentales cambios legislativos en la normativa sobre protección de datos, así como de la creciente evolución tecnológica; y, de otra, como señalábamos, considerando las determinaciones que se están produciendo en el ámbito de la protección de datos personales, y en los datos de salud, como consecuencia de la epidemia de COVID-19.

Así, para ello, determinaremos:

1º.- Que, tratándose de datos de salud, nos encontramos ante un tipo singular de datos personales, con unas características particulares que los hacen diferenciarse de los generales; los cuales poseen un contenido distinto y diferenciado, atribuyendo a su titular derechos diferenciados de los propios de los datos generales, e incluso de los demás datos incluidos dentro de la categoría de datos especialmente protegidos,

2º.- Que, la incidencia de la nueva regulación en la materia, ha supuesto una mejora en la protección de los datos de salud, en comparación con la normativa anterior que, como veremos, será necesario invocar en numerosas ocasiones como pauta, o directriz a falta de regulación aplicable al caso concreto.

III. ESTRUCTURA Y METODOLOGÍA

Partiendo del objeto principal del estudio, que es el estudio de los datos personales en el ámbito de la salud, entiendo que para llegar a analizar todo el campo de posible actuación de los datos de salud, resulta necesario, además del examen del marco general del sistema de protección de datos y de las especificidades que aportan los datos sanitarios o de salud, conforme a los dos fases indicadas anteriormente, abordar el estudio de los posibles contenidos en datos personales y datos de salud derivados de las obligaciones de publicidad, tanto activa (transparencia pública), como pasiva (derecho de acceso a la información); y, por tanto, determinar y analizar:

1.- Por un lado, la incidencia de datos personales de salud en la publicidad realizada en los Portales sanitarios de las CCAA y del Ministerio de Sanidad, Servicios Sociales e Igualdad, en la medida en que, mediante la publicidad de los elementos básicos de la publicidad, la transparencia en el ámbito sanitario juega un papel esencial, al permitir la planificación y evaluación del SNS por las administraciones sanitarias, así como la rendición de cuentas en la gestión; propiciando la posibilidad de exigir responsabilidades;

2.- Y, de otro, la materialización del derecho de acceso a la información en poder de las administraciones públicas, como traslación de su derecho constitucional y como elemento esencial en la mejora del sistema sanitario, derivada de la información resultado del acceso por los ciudadanos y la posibilidad de éstos de actuar en beneficio del sistema.

Sin embargo, hay que señalar que este objetivo de la transparencia sanitaria, ha quedado en entredicho como consecuencia de la pandemia de COVID-19, por cuanto en la declaración del estado de alarma quedó en suspenso el Portal de Transparencia sanitario de la Administración del Estado, así como los posibles accesos a información pública de salud de carácter estatal; provocando las quejas, sobre todo de periodistas y ciudadanos en general, en relación con los datos de la epidemia, ante la confusión provocada por la emisión de datos (sobre todo de personas fallecidas) que no contrastaban con los facilitados por las CCAA.

En el ámbito sanitario, la transparencia juega un papel esencial, en la medida en que los datos de contenido sanitario permiten, por parte de las administraciones, planificar y evaluar el funcionamiento del Sistema sanitario y rendir cuentas sobre su gestión,

mediante la necesaria publicidad de los elementos básicos de la actuación pública; lo que propicia lo posibilidad de ejercer responsabilidades, ya que de sus principios y reglas normativas participan de forma esencial los datos de salud, como categoría especial de los datos generales.

Del mismo modo, el acceso a los datos de salud constituye un elemento esencial en la mejora del sistema sanitario, por cuanto la información resultante del acceso por los ciudadanos permite que puedan actuar activamente mejorando la eficiencia del sistema; al mismo tiempo que, en la esfera particular, suponen un elemento esencial para la promoción y mejora de la salud de las personas, partiendo de que los datos clínicos de un paciente son el instrumento que utiliza el profesional médico para emplearlos en su proceso curativo.

Para ello, a la luz de la jurisprudencia, la novedosa legislación y principios de la protección de datos, además de las opiniones de la doctrina científica y las muy valiosas interpretaciones de las autoridades de control y de los Consejos de Transparencia (tanto nacional como autonómicos) hemos partido del análisis lógico de qué supone o en qué consiste la protección de datos, así como su reconocimiento constitucional y legal; para, después examinar como se materializa esta protección en todo el conjunto de operaciones o procedimientos que constituyen el tratamiento de datos, dentro del cual se ha tratado la problemática derivada de la transparencia, en cuanto al acceso a la información pública sanitaria y su reutilización, en la medida en que si contiene datos de carácter personal supone una limitación a su comunicación.

Estructura del trabajo

Entiendo que el contenido propiamente jurídico-administrativo de este trabajo de investigación justifica que la mejor división estructural del mismo, conforme a su naturaleza, sea la de división en epígrafes y, en su caso, derivaciones o aportados de los mismos, mediante subepígrafes.

De esta forma, el trabajo se estructura en dos grandes apartados: El Sistema de protección de datos (PARTE I) y la protección de datos y la transparencia y acceso a la información pública sanitarias (PARTE II). A su vez, cada uno de los dos apartados (I y II) se

estructuran en capítulos; los cuales a su vez se dividen en epígrafes y, en su caso, en su subepígrafes.

Así, la estructura del trabajo gira entorno a estos dos grandes apartados:

PARTE I.- En el que se aborda el conjunto del Sistema de protección de datos (y, por tanto) de los datos de salud, a su vez estructurado entorno a dos capítulos:

1.- Capítulo I, el derecho a la protección de datos, en el que se analiza el estudio del derecho a la intimidad como objeto de la protección de datos, y el *iter* histórico de cómo se llega al reconocimiento de este derecho: desde sus precedentes internacionales y europeos hasta llegar al reconocimiento constitucional y legal (europeo y nacional). Como elemento imprescindible del adecuado funcionamiento del sistema de protección de datos están las garantías incluidas en el propio sistema que se ejercen por las autoridades de control independientes; tanto nacional o autonómicas, como europea. A ello, se une un sistema sancionador, como elemento esencial del sistema, contenido en el RGPD, y complementado en la LOPDGDD.

2.- Capítulo II, relativo al examen de los datos personales en el ámbito de la salud, en el que se incluye los caracteres que delimitan este tipo de datos respecto de los demás datos personales y su característica de especial sensibilidad y necesaria confidencialidad y secreto por parte de los profesionales, tanto sanitarios como no sanitarios.

Se aborda también, como se ponen de manifiesto, los posibles conflictos de invasión de la privacidad de los datos de salud a través del tratamiento y cesión de los mismos, tanto en la normal asistencia sanitaria como en actuaciones indirectas, como los seguros de salud.

En este apartado, como elementos fundamentales del sistema de protección de datos se incluyen los principios aplicables al tratamiento de los datos de salud y los derechos de los titulares de datos que pueden afectar a datos de salud; incluyendo el acceso a la HC, tanto por el propio paciente como por las personas o entidades autorizadas legalmente: el profesional sanitario, administraciones sanitarias, órganos judiciales y determinados órganos constitucionales. Este acceso, además de su elemento natural que es el territorio nacional, puede producirse fuera de nuestras fronteras, como consecuencia de una asistencia sanitaria transfronteriza.

Elemento esencial que delimita que el tratamiento de datos que se lleva a cabo sea lícito es su legitimación: además del consentimiento y otras bases legitimadoras. Así, el art. 9.2 RGPD contiene otros supuestos de licitud del tratamiento de datos de salud (de categorías especiales de datos personales), que se excepcionan de la prohibición de tratamiento de estos datos del art. 9.1 RGPD: apartado 2, b), c), e) y g).

Se incluyen como elemento, también importantes del sistema, la seguridad y protección de los datos de salud.

PARTE II.- Se refiere a la interacción existente entre la protección de datos y la transparencia y acceso a la información pública sanitarias, dirigido a analizar el contenido de la información pública, en la medida en que pueda contener datos personales o de salud; bien se trate de la publicidad activa o transparencia, como elemento esencial de participación de los ciudadanos en la salud (capítulo 1) como la pasiva, derivada del ejercicio del derecho de acceso a la información pública (capítulo 3); determinada por el análisis, de la aplicación al caso concreto de solicitud de acceso, del límite que constituye que en el contenido de dicha información existan datos personales y de los datos de salud. Además, se analiza la problemática de la utilización de las nuevas tecnologías aplicadas a la salud en cuanto a su afectación a la protección de datos de salud. (capítulo 2).

Metodología

Fijado nuestro objetivo de demostrar la singularidad de los datos de salud respecto del conjunto de datos de carácter general, incluso, del resto de datos de categorías especiales; y, por tanto, esta especificidad lleve aparejada; de una parte, una diferente consideración en cuanto al tratamiento de los datos de salud, y, por tanto, con un régimen especial, o para determinadas situaciones (que no constituyan tal régimen), que asignen derechos diferenciados a los titulares de datos de salud, en relación con el régimen general; además, de determinar, implícitamente, como estas especificidades de los datos de salud, se producen a la luz de la nueva normativa sobre protección de datos, en relación con la anterior, hemos considerado que, para conseguir los resultados previstos, la mejor forma era centrándonos en los aspectos prácticos de la asistencia sanitaria y de la práctica

clínica, tal como se desarrollan en nuestro SNS, que asigna su competencia a las CCAA, desde un enfoque descriptivo y crítico[1].

Así, si realizamos un análisis que parte de lo superior a lo inferior (el paciente), nos encontramos (como primer nivel) con el funcionamiento y organización del sistema sanitario y, en concreto, de la información pública de carácter sanitario, comprensiva tanto de grandes cifras o elementos, como pueden ser datos epidemiológicos o la construcción de complejos hospitalarios, a listas de espera quirúrgicas o el acceso a subvenciones públicas para colectivos de personas con determinadas patologías. Dentro del ámbito de la información, habría que diferenciar lo que constituye información al paciente con carácter previo a una actuación de contenido sanitario (consentimiento informado), de aquella exigida por el RGPD para llevar a cabo el tratamiento de datos de salud, como elemento de control de sus propios datos por parte del titular afectado.

El siguiente escalón, podríamos encontrarlo también en el propio funcionamiento del sistema sanitario en cuanto a las condiciones de seguridad en las que se producen los datos de salud (centros sanitarios, normalmente). En este caso, si partimos de que la seguridad de los datos personales un elemento fundamental en el sistema de protección de datos; tratándose de datos de salud, la trascendencia, si cabe, es todavía mayor, habida cuenta de la alta sensibilidad que tiene el contenido de los datos de salud. Por ello, hemos entrado a examinar como se realizan las medidas de seguridad en los recintos sanitarios, señalando las posibles brechas de seguridad, así como aquellas actuaciones que vulneran la intimidad de los pacientes y que (todavía) siguen existiendo. Además, de incluir distintas recomendaciones en evitación de posibles afectaciones a la privacidad de los pacientes.

En este mismo apartado, incluiríamos lo que hemos venido a llamar "reutilización de los datos de salud", o más bien, de la información en salud; destacando el examen de como aquellas herramientas tecnológicas utilizadas en la asistencia sanitaria vienen a contener, en su utilización para el paciente (tratamiento de información), elementos que pueden afectar a la intimidad del paciente o usuario sanitario; en la medida en que, a mayor tecnificación mayor es la posibilidad de afectación de datos de salud. Así, en el empleo

[1] Para una mejor comprensión de la organización del SNS, vide HERNÁNDEZ BEJARANO, M., La Ordenación sanitaria en España, Edit, Thomson-Civitas, Pamplona, 2004.

de la telemedicina como herramienta sanitaria lleva incorporado la necesidad de cumplimiento de un riguroso protocolo de identificación y aceptación; ya que, de otra forma, podrían afectarse datos sensibles de las personas.

En el último escalón, encuadraríamos todo aquello relacionado con la protección de los datos de salud para un paciente concreto, como usuario del sistema sanitario. Así, examinamos los principios y derechos de los titulares de salud como consecuencia del tratamiento de sus datos en la asistencia sanitaria, poniendo de manifiesto las particularidades con relación al tratamiento general de datos y la problemática práctica que presentan; señalando como, para los datos de salud no basta el consentimiento del paciente para el tratamiento de estos datos, sino que es necesario que exista una ley habilitante previa.

Destacamos, el estudio del régimen de acceso por el paciente a sus datos de salud, en concreto a su HC, indicando la problemática que se plantea en la realidad. Al mismo tiempo que, como uno de los objetivos de la tesis, analizamos la problemática derivada de la confrontación entre el acceso a los datos de salud y, por tanto, de la prestación de la asistencia sanitaria y la necesaria protección y garantías de estos datos.

Este acceso a los datos de salud que, no solamente puede llevar a cabo el paciente, sino que (por habilitación legal y con las cautelas establecidas) pueden llevarlo a cabo los profesionales sanitarios, las Administraciones sanitarias y los órganos judiciales y constitucionales (determinados); teniendo, además de su lógica dimensión nacional, una internacional, en la medida en que puede haber tratamiento de datos de salud debido a que el paciente se traslada a un país europeo y necesita asistencia sanitaria; planteándose, por ello, una problemática especial que analizamos igualmente.

Por último, en el ámbito del acceso a los datos de salud, nos encontramos con aquella información pública que una persona puede solicitar a un organismo público que está en su poder, en virtud del derecho de acceso a esta información, y en cuyo contenido pueden existir datos personales y, en concreto, datos de salud. Así, analizamos su problemática a la luz de la legislación, la jurisprudencia, las opiniones doctrinales y de la casuística, sobre la base de las resoluciones e informes de la AEPD y del Consejo de Transparencia, tanto nacional como de las diferentes autonomías.

Medios y recursos

El material empleado en el desarrollo de este trabajo está compuesto por el siguiente material relacionado con el ámbito de este trabajo:

a) Material normativo, en su distinta jerarquía y forma y en sus distintos ámbitos, tanto nacional o autonómico, como europeo (de la UE o fuera de ella) o internacional. Se incluyen los proyectos normativos. Con profusión de citas a pie de página se incluye esta normativa utilizada, que en determinadas ocasiones incluye el contenido concreto del precepto de que se trata.

b) Material jurisprudencial que, a nivel nacional, incluye todos los niveles jurisdiccionales; europeo, a través de las sentencias del TJUE; e internacional, mediante sentencias del TEDH o del TPI. Se incluyen, en particular, sentencias propias de la Jurisdicción Contencioso-Administrativa recaídas en casos de acceso a información pública o derivadas de una resolución impugnada de la AEPD.

c) Material doctrinal, contenida tanto en material bibliográfico como en artículos y revistas, incluidos o no en colecciones legislativas, y accesibles tanto documentalmente como electrónicamente. Estas aportaciones han sido de una valiosa aportación para la ejecución del trabajo, aportando luz y visión crítica a cuestiones diversas.

d) Aquí, incluimos como fuente de extraordinaria importancia la derivada; tanto de las autoridades de control, tanto nacional o autonómicas, como el supervisor europeo, y de los Consejos de Transparencia; igualmente, nacional y autonómicos.

e) Otras fuentes, como pueden ser noticias en medios periodísticos u otras fuentes, generalmente accesibles desde Internet.

PARTE I

LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA SALUD

CAPÍTULO I

EL DERECHO A LA PROTECCIÓN DE DATOS

1. EL DERECHO A LA PROTECCIÓN DE DATOS

1.1. EL DERECHO A LA INTIMIDAD COMO OBJETO DE LA PROTECCIÓN DE DATOS

1.1.1. ÁMBITO CONSTITUCIONAL. DELIMITACIÓN DE SU CONTENIDO ESENCIAL

Como paso previo al estudio de los datos personales en el ámbito sanitario, es preciso referirse al derecho a la intimidad como elemento esencial de la persona y, por tanto, objeto de la protección de datos personales. Así, veremos, como se ha producido una transformación del derecho a la intimidad, al pasar de una idea de protección de lo más interno de la persona a otra en la que se amplía su marco de protección para incluir el poder de disposición o control del titular de los espacios propios de su esfera más íntima en la medida en que tienen una proyección al exterior.

La CE consagra de forma expresa el derecho a la intimidad como derecho fundamental, derivado de la propia dignidad humana y vinculado íntimamente con la propia personalidad[2]. Así, el TC acoge el derecho a la intimidad, diferenciando entre los derechos a la intimidad, honor y propia imagen en un mismo artículo –art. 18.1- en el que se incluyen distintos apartados comprensivos de sus manifestaciones: inviolabilidad del domicilio y secreto de las comunicaciones –apdos.2 y 3, y el derecho a la

[2] Sin embargo, nuestra constitución no menciona la dignidad humana, sino la dignidad de la persona, como señala GUTIÉRREZ GUTIÉRREZ, I., *Dignidad de la persona y derechos fundamentales*, Marcial Pons, Madrid, 2005, p. 85.

autodeterminación informativa –apdo.4-. Además, recoge el derecho a la información y el secreto profesional en el art. 20.1., apartados. a) y d).

Se trata de derechos que representan la máxima expresión de la dignidad humana de los que no es posible renunciar sin que afecten a la condición de la persona, integrados dentro de los derechos de personalidad, como señala el TC "(…) *aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la «dignidad de la persona», que reconoce el art. 10 de la C.E., y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario - según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana. Se muestran así esos derechos como personalísimos y ligados a la misma existencia del individuo (…)*[3]*"*

La jurisprudencia constitucional ha evolucionado, partiendo de una concepción inicial del derecho a la intimidad como un derecho negativo de defensa y no intromisión en la vida privada[4] de la persona ha pasado a una idea más activa y positiva de este derecho en el que se incluye además un poder de disposición o control de la persona sobre el contenido de toda la información reservada de su esfera personal y familiar. Así, altera la configuración del derecho a la intimidad, al entender que el art. 18.1 CE: *"no garantiza una intimidad determinada, sino el derecho a poseerla"*, y al mismo tiempo disponer de:

> *"(…) un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público (…) vedando que terceros, sean particulares o poderes públicos, decidan cuáles son los lindes de nuestra vida privada pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea el contenido del espacio.*
>
> *Del precepto constitucional se deduce que el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a su persona o a la de su familia, pudiendo imponer a terceros su voluntad de no dar a conocer dicha información o prohibiendo su difusión consentida (…)"*[5]

[3] STC 231/1988, de 2 de diciembre, FJ 3.
[4] STC 73/1982, de 2 de diciembre, FJ 5.
[5] STC 134/1999, de 15 de julio, FJ 5.

En la posterior STC 231/1988, el TC[6] aborda la existencia de dos tipos de amenazas o peligros: la posibilidad de intromisión de una esfera o ámbito íntimo o propio y su exteriorización o conocimiento externo de la información de los hechos producidos en este ámbito reservado. Así, los derechos a la imagen, y a la intimidad personal y familiar "*se muestran como derechos personalísimos y ligados a la existencia misma del individuo…".* Por tanto, se trata de un derecho inherente a la persona, y derivado de la propia dignidad humana, al tratarse de un derecho de la personalidad. Posteriormente, ha evolucionado hacia una interpretación amplia del contenido del derecho a la intimidad vertida en la STC 196/2004, de 15 de noviembre, en la que se recoge toda la doctrina constitucional entorno al derecho a la intimidad como derecho fundamental garantizado en el art. 18.1.:

> "(…) *Debe estimarse que, en principio, el derecho a la intimidad personal y familiar se extiende, no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen. ... Por lo que existe al respecto un derecho -propio, y no ajeno- a la intimidad, constitucionalmente protegible*" (FJ 4).

La importancia de esta sentencia radica en que viene a reconocer el derecho a la "*privacy"*, a la vida privada, de forma que se amplía el contenido inicial del art. 18.1 CE para incluir junto a la vida privada de la persona a la de su familia[7]. Así, incluiría, además de lo íntimo, todo el conjunto que integra la vida privada y familiar de una persona; que sería lo que denominamos privado, definido como aquel espacio que no es público, y en el que tienen lugar las relaciones interpersonales, de afecto amistad, etc.[8]. Esta sería la postura del TC, para el que el derecho a la intimidad *"(…) limita la intervención de otras*

[6] STC 231/1988, de 2 de diciembre, FJ 3.
[7] SUÁREZ RUBIO, M.J., *Constitución y privacidad sanitaria*, Tirant Lo Blanc, Valencia, 2017, p. 53, con cita de DÍEZ-PICAZO GIMÉNEZ, L.M., en su libro *Sistema de Derechos fundamentales,* Thompson, Madrid, 2013, pp. 41 y 42.
[8] FERNÁNDEZ-RUIZ GÁLVEZ, E., "Intimidad y confidencialidad en la relación clínica", *Servicio de Publicaciones de la Universidad de Navarra,* Persona y Derecho, Vol. 69, Pamplona, 2013, pp. 61-63.

personas y de los poderes públicos en la vida privada, y excluye las intromisiones de los demás en la esfera de la vida personal y familiar de los ciudadanos"; según se indica en la STC 117/1994, de 25 de abril, F.3 (caso Ana Obregón), y otras, que veremos a continuación.

En una concepción subjetiva utilizada por el TC en distintos fallos, atribuye a la persona su total disponibilidad de lo que tiene que quedar o no reservado para las intromisiones de terceros, consintiéndolo en caso contrario. De forma que la privacidad se concibe como una libertad positiva para ejercer un derecho de control sobre los datos de la propia persona que han salido de la esfera de la intimidad para convertirse en un archivo electrónico[9].

Sin embargo, el contenido del derecho a la intimidad no es lo fundamental, sino que lo trascendente es el derecho a poseerla: "

> *"(...) De suerte que el derecho a la intimidad (...) no garantiza una intimidad determinada sino el derecho a poseerla, disponiendo a este fin de un poder jurídico sobre la publicidad de la información relativa al círculo reservado de su persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público (...)"*[10].

No obstante, el derecho a la intimidad tiene sus límites, al igual que sucede con todos los derechos fundamentales, en cuanto tienen un significado especial para el desarrollo de la personalidad y la dignidad humana mantienen un reservado un contenido esencial, indisponible e irrenunciable, que no puede ser vulnerado por el legislador sin vulnerar la Constitución. Así, lo pone de manifiesto el TC al señalar:

> *" (...) en relación a los derechos fundamentales, establece la Constitución por sí misma en algunas ocasiones, mientras en otras el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad*

[9] STC 142/1993, de 22 de abril, FJ 7.
[10] STC 99/2002, de 6 de mayo, FJ 6. El párrafo es literalmente copiado o repetido por la STC 121/2002, de 20 de mayo, en su FJ 2.

de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos"[11].

1.1.2. LA PROTECCIÓN DE DATOS COMO DERECHO AUTÓNOMO FRENTE A LA INTIMIDAD

La protección de datos constituye un derecho autónomo e independiente, cuyo objeto en la LOPD[12] es la intimidad, pero entendida, no en un sentido de protección de lo íntimo y reservado de la persona, sino en un sentido amplio y global, en el que se incluyan aspectos relacionados con el honor y la intimidad[13]. Y esta protección se extiende, además de a la intimidad, a los datos de carácter personal, a la información personal, tengan o no carácter íntimo, incluyendo los datos personales de carácter público:

> *"(...) el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal".*
>
> *"También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"[14].*

[11] STC 2/1982 de 29 de enero FJ 5. Así mismo, la STC 11/1981 de 8 de abril, y STC 156/2001 de 2 de julio.
[12] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[13] SERRANO PÉREZ, M.M, *El derecho fundamental a la protección de datos. Derecho español y Comparado*, Aranzadi, Pamplona 2004, pp. 33 y ss.
[14] STC 292/2002, de 30 de noviembre, FJ 6.

La privacidad supone un concepto más amplio que el de la intimidad, que incluiría el conjunto de aspectos relacionados con la personalidad del individuo que son objeto de reserva; mientras la intimidad constituiría una de las facetas de la vida privada de ámbito más limitado y reservado de la vida privada. De esta forma, la privacidad vendría a configurarse como "derecho de la personalidad", en el que se incluirían los datos personales, de carácter íntimo o no.

La jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) se ha encargado de delimitar el contenido de "vida privada", deslindando sus tres ámbitos de desarrollo:

1º.- El derecho a la defensa de su vida privada, como núcleo central de las garantías del art. 8 CEDH[15], y en el que se incluiría:

a) La comunicación verbal con otras personas.

b) El derecho a la propia imagen y al honor personal como partes integrantes de la esfera privada, al tratarse de manifestaciones directas de la dignidad de la persona.

c) Respeto del nombre y apellidos como aspectos de la identidad personal y como nexo de unión con la familia[16].

d) Ante los avances de las nuevas tecnologías y los peligros de la informática sobre la privacidad personal, la defensa de los datos personales se ha convertido en un elemento fundamental para garantizar la vida privada de los individuos. Por ello, la protección de datos, y en especial, los de carácter sanitario, se consideran como parte del derecho del respeto a la vida privada.

2º.- El derecho a la autodeterminación corporal, en el que se incluye la integridad tanto física como psíquica del individuo, como elementos integrantes de su ámbito o esfera de privacidad. Este derecho se manifiesta en el ámbito sanitario en la necesaria prestación del consentimiento del paciente previo a cualquier actuación médica que afecte a su

[15] Convenio para la protección de los derechos humanos y las libertades fundamentales, de 4 de noviembre de 1950.
[16] SSTEDH de 22 de febrero de 1994, caso *Burghartz; y* de 25 de noviembre de 1994, caso *Stjerna*, entre otros.

ámbito corporal o psíquico. Además, incluiría el derecho genérico de toda persona a poder determinar su vida sexual, comprendiendo la libertad de relaciones sexuales e incluso sadomasoquistas[17].

Este derecho puede conectarse con el derecho a la vida y con la prohibición de cualquier tipo de tortura o tratos inhumanos y degradantes, reconocidos en los arts. 2 y 3 del CEDH, respectivamente.

3º.- Derecho al libre desarrollo del estilo de vida, que a su vez integraría los siguientes derechos:

a) Respeto a las relaciones interpersonales, tanto en el ámbito personal y familiar como comercial y laboral[18];

b) La defensa del medio ambiente como ámbito necesario para el desarrollo de la vida familiar y privada;

c) Protección especial para la forma de vida de las minorías, que tiene su apoyo general en el art. 14 CEDH, que excluye cualquier discriminación;

1.1.2.1. Diferencias entre ambos derechos

En cuanto al contenido, el derecho a la intimidad implica una limitación de abstenerse de entrar en cualquiera de sus facetas; frente al derecho a la protección de datos, en el que su titular está en posesión de un conjunto de facultades que implican obligaciones jurídicas para las terceras personas que operan con los datos personales, que se manifiestan como deberes jurídicos de hacer.

Así, a diferencia del derecho a la intimidad, el objeto de la protección de datos abarca, no sólo a la protección de los datos íntimos personales *"(…) sino a cualquier tipo de dato*

[17] Relacionado con este tema, SSTEDH de 22 de octubre de 1981, caso *Dudgeon* y 26 de octubre de 1988, caso *Norris*. Sin embargo, encontramos opiniones contrarias como la del Juez Pettiti en el caso *Laskey Jaggard*, sentencia de 19 de febrero de 1997.

[18] Para el TEDH no es posible separar el ámbito personal del laboral. SSTEDH de 16 de diciembre de 1992, caso *Niemietz y* 16 de diciembre de 2000, caso *Amann.*

personal, sea íntimo o no, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos", incluyendo cualquier dato que permita identificar a una persona y relacionarse con una concreta identidad personal *"(…) aquellos datos que identifiquen o permitan la identificación de la persona, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"*[19].

La diferenciación entre los derechos de intimidad y derecho a la protección de datos se pone de manifiesto con mayor intensidad en la STC 292/2000, de 30 de noviembre, señalando que radica en "*su distinta función, lo que apareja que su objeto y contenido difieran"*[20]. Así, aunque comparten un mismo objetivo, el de garantizar la vida privada personal y familiar; mientras el derecho a la intimidad tiene como función la protección del ámbito o esfera íntima o personal frente a intromisiones externas, "(…) *el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derechos del afectado*"[21]

De esta forma, el objeto del derecho a la protección de datos, diferente al del derecho a la intimidad,

> "(…) *amplia la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de las personas, sean o no constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado*".

Por su parte, el objeto de la autodeterminación informativa no se reduce sólo a la protección de los datos íntimos personales, sino que se extiende a:

---

[19] STC 292/2000, de 30 de noviembre, FJ 6.

[20] Así lo pone de manifiesto GARRIGA GONZÁLEZ, Ana, citando a DENNINGER, E., "El derecho a la autodeterminación informativa", en PÉREZ LUÑO, A., E., *Problemas actuales de documentación y la información jurídica,* Tecnos, Madrid, 1987, p. 273., vide, asimismo, CONDE ORTIZ, C., *La protección de datos personales. Un derecho con base en los conceptos de intimidad y privacidad*, Dykinson, Madrid, 2005.
Sobre la autodeterminación informativa, véase así mismo, PIÑAR MAÑAS, J.L."Protección de datos: origen, situación actual y retos para el futuro", en PIÑAR MAÑAS, J.L., *El derecho a la autoderminación informativa,* Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 84 y ss.

[21] STC 292/2000, FJ 6.

> *"(…) cualquier tipo de dato personal, sea íntimo o no, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objetivo no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal (…)*"[22].

Por tanto, se considera dato personal cualquier tipo de dato que permita la identificación de una persona; es decir que a través del dato pueda relacionarse con una determinada identificación personal, ya que mediante este dato es posible " (…) *servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier índole, o (…) para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo*". Por ello, la protección se extiende, incluso, hasta los datos públicos, que pudiendo ser posible su acceso por cualquier persona " (…) *no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos*"[23].

Si nos fijamos en la función que realizan ambos derechos; mientras el derecho a la intimidad tendría un carácter negativo o defensivo, dirigido a proteger la vida personal y familiar ante las intromisiones externas[24], el derecho a la protección de datos tendría una finalidad positiva o de actuación, dirigida a garantizar un poder de control o de disposición del titular sobre sus datos personales.

[22] STC 292/2000, FJ 6.
[23] *Ibid.*
[24] "El derecho a la intimidad salvaguardado en el art. 18.1 C.E. tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean estos poderes públicos o simples particulares, que está ligado al respeto de su dignidad (SSTC 73/1982, 110/1984, 107/1987, 231/1988, 197/1991, 143/1994 y 15/1997). (…) el art. 18.1 C.E. no garantiza sin más la "intimidad", sino el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea cual sea el contenido de aquello que se desea mantener al abrigo del conocimiento público. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías, y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con que fin*" (*Por todas, STC 144/1999, de 22 de julio, FJ 8).

1.2. RECONOCIMIENTO DEL DERECHO A LA PROTECCIÓN DE DATOS

1.2.1. PRECEDENTES NORMATIVOS Y JURISPRUDENCIALES INTERNACIONALES Y EUROPEOS

Las normas y principios jurisprudenciales que ahora examinamos fueron determinantes en la definición de la construcción del contenido del derecho a la protección de datos personales. Resaltar, como el reconocimiento de este derecho es el resultado de la actividad jurisprudencial del TJCE, que reconoce la existencia a la protección de datos personales (configurando alguno de sus elementos principales) y del papel fundamental desempeñado por las instituciones europeas mediante la elaboración normativa[25], unido a las influencias recíprocas entre los ordenamientos nacionales y los ordenamientos jurídicos de carácter supranacional: Consejo de Europa, a través del Convenio Europeo de Derechos Humanos, y el ordenamiento propio de la UE.

La definición contenida en el Convenio 108[26] y luego incluida en la Directiva 94/56, ha sido la manejada por el TEDH, de forma que se entiende por datos personales "cualquier información relativa a un individuo identificado o identificable"[27], no sólo referidos a la vida privada sino a la vida pública, siempre que afecte al desarrollo de su personalidad.

[25] En concreto la Directiva 97/66/CE, sobre Protección de Datos y Telecomunicaciones, encargada de regular la protección de datos personales en este sector, que fue derogada por la Directiva 2002/58/CE, sobre Protección de Datos y Comunicaciones Electrónicas, también derogada. Ambas directivas tenían como fundamento la Directiva 95/46/CE sobre Protección de Datos Personales a estos dos sectores concretos. Además, el Reglamento 45/2001, vino a sustituir la regulación que esta Directiva hacía de la protección de datos en las instituciones europeas; y además se crea el "Supervisor Europeo de Protección de Datos", como órgano específico de protección de los datos personales, dotado de una garantía específica y reforzada (http://www.europarl.europa.eu).

[26] "Artículo 8. Garantías complementarías para la persona concernida.
Cualquier persona deberá poder:
a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;
b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;
c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;
d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, que se refieren los párrafos b) y c) del presente artículo".

[27] STEDH de 16 de febrero de 2000, caso *Amann* y 4 de mayo de 2000, caso *Rotaru*.

De lo que resulta que el contenido y límites de este derecho depende tanto del tipo de datos como de su utilización[28]; delimitando, al mismo tiempo, una parcela de datos personales de carácter "sensible", para los que se exige una protección reforzada.

Aunque inicialmente el TEDH no utiliza la expresión de "protección de datos personales", será a partir del caso *Leander*[29] cuando de forma expresa reconozca la existencia de este derecho como parte del derecho a la vida privada reconocido en el art. 8 del CEDH[30], que reconoce a toda persona el "derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia", como derechos de carácter personalísimo ligados a la propia existencia del individuo; siendo su objetivo la protección de la esfera privada del individuo, a través de estos cuatro ámbitos de protección: la vida privada, la vida familiar, el domicilio y la correspondencia.

En cuanto a la vida privada, el CEDH la entendió inicialmente como contraposición a la vida pública para posteriormente, a través de la jurisprudencia del TEDH, en una interpretación más extensa, entender no sólo la garantía de una esfera interna de la personalidad, sino que se protege también el derecho a la intimidad y el desarrollo personal y el derecho a establecer y desarrollar relaciones con otras personas y con el mundo exterior; éste último, incluiría actividades de naturaleza profesional o comercial, como resultado de una interpretación amplia del concepto de "hogar" y de "vida privada". Así, el ámbito de la vida privada estaría delimitado por todo aquello que constituyen relaciones del individuo con otras personas, con el fin de desarrollar su personalidad[31].

Los titulares del derecho (de protección de datos), reconocido en el art. 8 CEDH, son las personas físicas, se incluyen a los menores de edad que pueden ejercerlo sin consentimiento de su representante. Respecto de las personas jurídicas se reconoce una titularidad matizada; por cuanto no opera respecto de derechos de carácter personalísimo, como el derecho a la vida y el respeto a la vida familiar, pero si se admite que puede

[28] STEDH de 7 de julio de 1989, caso *Gaskin*.

[29] En este caso, fue cuando por primera vez se consideró como la recogida de datos personales lesionaba la vida privada de la persona. STEDH de 26 de marzo de 1987, caso *Leander*.

[30] Como inspiración del art. 12 de la Declaración Universal de Derechos Humanos y del art. 17 del Pacto Internacional de Derechos Civiles y Políticos.

[31] En la propia sentencia se recurre a la cita de las SSTEDH de 12 de julio de 1977, caso *Brüggeman and Scheuten*; y de 24 de julio de 2003, caso *Smirnova*.

invocarse cierta protección respecto a las escuchas telefónicas y el respeto al domicilio y correspondencia[32].

En cuanto a los obligados por este derecho, hay que partir de que el propio art. 8 CEDH tiene como finalidad proteger al individuo frente a las intromisiones del poder público en su vida privada y familiar. De ahí, que sean los poderes públicos los principales obligados por este derecho, aplicándose el CEDH no sólo a las relaciones entre poderes públicos y particulares, sino también a las relaciones entre particulares; aunque únicamente el TEDH reconoce un efecto horizontal[33] indirecto del derecho a la vida privada en las relaciones entre particulares.

Para el TEDH el derecho a la protección de datos personales, como integrante del derecho más general a la vida privada se trataría, no solamente de un derecho de defensa o pasivo, sino que también tendría consistiría en un derecho proactivo o de prestación, cuyo contenido iría, además, dirigido a la exigencia de determinadas actuaciones positivas a los obligados al mismo[34].

De esta forma, las facultades protegidas por el derecho a la protección de datos serían las reconocidas en el Convenio 108 (arts. 5 y 8), y así se puso de manifiesto por primera vez en el caso *Klass*[35] al reconocer estas facultades:

a) derecho de información, derecho a ser informado;

b) derecho a la libre disposición de los datos: consentimiento del titular de los datos después de haber sido informado de la recogida y tratamiento de los datos personales y su utilización para la finalidad prevista, así como para la cesión o comunicación a terceros;

c) derecho de acceso, para que el titular de los datos pueda conocer qué y cómo han sido almacenados sus datos; aunque el TEDH no reconoce un derecho de acceso general de

[32] Puede verse la interpretación favorable en este sentido plasmada en el caso *Stés Colas Est*, STEDH de 16 de abril de 2002.

[33] La eficacia horizontal de los derechos fundamentales fue construida a raíz de la defensa de la dignidad humana de la Ley Fundamental alemana.
El llamado "efecto horizontal" (o "*Drittwirkung"*) del CEDH, ha sido reconocido entre otras por la SSTEDH de 24 de febrero de 1998, caso *Botta*, y 13 de febrero de 2003, caso *Odiévre*.

[34] ARENAS RAMIRO, M., *El Derecho Fundamental a la Protección de Datos Personales en Europa*. *Monografías*, Tirant lo Blanch, Valencia, 2006, pp. 95 y ss.

[35] STEDH de 6 de septiembre de 1978.

acceso a la información, garantizado por el art. 8 CEDH, sino que dependerá de cada caso concreto[36];

d) derecho de rectificación y cancelación o "borrado", considerando la finalidad de la recogida de los datos y su conservación.

Sin embargo, como todos los derechos, los derechos reconocidos en el art. 8 CEDH no son derechos absolutos, pudiendo ser objeto de restricciones o injerencias por parte de los poderes públicos, como señala el art. 8.2 CDHE[37]; debiendo estos casos de excepción de la regla general del art. 8.1 interpretarse de forma restrictiva. Así, los límites establecidos en el art. 8.2 parten de los límites contenidos en el art. 29.2, siendo similares a los recogidos en los arts. 9 a 11 CEDH que reconocen otros derechos fundamentales.

La manifestación concreta de estas limitaciones se lleva a cabo a través de las llamadas "injerencias públicas", cuyas condiciones para su validez son las siguientes:

- *Establecimiento mediante ley*. En cuanto a las injerencias respecto del ámbito de protección brindado por el art. 8C CEDH, sólo pueden entenderse justificadas si se establecen mediante ley material y no formal, sin permitirse analogías[38], debiendo, además, cumplirse los requisitos de accesibilidad y previsibilidad, exigidas por el TEDH[39] con especial rigor en relación con los datos personales.
- *Finalidad legítima*, que justifique una injerencia de la autoridad pública en la vida privada. Injerencias reconocidas en el art. 8.2 CEDH: seguridad nacional, seguridad pública, bienestar económico del país, defensa del orden y prevención del delito, protección de la salud o de la moral y la protección de los derechos y libertades ajenos.
- *Proporcionalidad*. Este principio, por el cual se realiza una ponderación o medida entre el derecho afectado y el fin conseguido con la medida adoptada entre los

[36] STEDH de 7 de julio de 1989, caso *Gaskin*.

[37] "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

[38] STEDH de 22 de octubre de 2002, caso *Taylor-Sabori.*

[39] Es el supuesto de las escuchas telefónicas. SSTEDH de 27 de abril de 2004, caso *Doerga*, y de 31 de mayo de 2005, caso *Vetter*, entre otros.

> intereses individuales y los generales, ha tenido gran importancia en labor interpretativa del TEDH.

Es decir que la limitación de derechos tenga justificación suficiente, en el sentido de ser necesaria para atender a una urgente necesidad social. Así, como señala ARENAS RAMIRO[40], el test de "necesidad para una sociedad democrática" se lleva a cabo mediante el principio de proporcionalidad; de forma que el que la medida limitativa a realizar sea necesaria debe entenderse en el sentido de que suponga una "necesidad o exigencia social imperiosa"; debiendo previamente existir un motivo suficiente, ya que sino la medida no es necesaria y por tanto sería injustificada[41].

Recordar, como la primera sentencia[42] que resuelve un caso sobre datos personales data de 1969, siendo dictada por el TJCE, y reconociendo a los derechos fundamentales como integrantes del ordenamiento comunitario. De esta forma, el derecho a la protección de datos personales tiene una dimensión claramente internacional de la que no participan otros derechos fundamentales; de ahí, que nuestro derecho positivo y jurisprudencia hayan "bebido" de forma muy importante de todo el marco jurídico y jurisprudencial internacional.

Debemos considerar como el resurgimiento de este derecho se produce con la introducción de las nuevas tecnologías y el avance de la informática, que permiten la transferencia de bancos de datos no sólo a nivel nacional sino internacional. De ahí, que sea necesario resaltar como los riesgos de intromisión y sus correspondientes garantías tienen un carácter que excede de los ámbitos nacionales para pasar a ser de marcado carácter mundial.

[40] ARENAS RAMIRO, *op.cit.*, pp.119-131.
[41] STEDH de 26 de noviembre de 1991, caso *Chassagnou*.
[42] Caso *Stauder*. Asunto *STAUDER v. Stadt Ulm-Sozialamt* (29/69), de 12 de noviembre de 1969.

1.2.1.1. Convenio 108 y Directiva 95/46 CE

El Convenio del Consejo de Europa y la Directiva 95/46 han constituido la base de nuestra legislación de protección de datos, de ahí que tanto la LORTAD[43] como la actual LOPDGDD[44] estén ampliamente influenciadas por estos dos instrumentos jurídicos, a lo que hay que añadir la trascendencia que en ello han tenido las legislaciones de países europeos, en especial la alemana.

La Directiva 95/46[45] constituyó durante el tiempo que estuvo vigente hasta su derogación por el Reglamento General de Protección de Datos (RGPD)[46], la norma fundamental de carácter europeo sobre esta materia. La Directiva, se dictó con el doble objetivo de garantizar el derecho a la vida privada reconocido en el art. 8 CEDH, y en concreto en lo relativo a la protección de datos personales y el de impedir la restricción de la libre circulación de los datos personales, a través del reconocimiento de unos principios comunes para todos los Estados miembros.

La posición de la Directiva, coincidente con los planteamientos de las primeras sentencias del TJUE que la interpretan, es la de proteger los tratamientos para que no violen los derechos fundamentales y, en particular, el derecho a la intimidad[47].

De su trasposición surgió la LOPD[48], que se aplicaba a cualquier tipo de tratamiento de datos personales, automatizados o no, de forma que el tratamiento incluye desde la recogida hasta la difusión de la información; además de distinguir una categoría especial de datos, de los que se prohíbe su tratamiento salvo consentimiento expreso de su titular.

---

43 Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

44 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

45 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.

46 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).

47 PIÑAR MAÑAS, J.L., "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre Protección de Datos, pp. 45 y ss.

48 Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En el año 2003, el TJCE dicta de forma expresa las dos primeras sentencias[49] relativas a la interpretación de la Directiva 95/46/CE[50].

1.2.1.1.1. Convenio 108

El Convenio 108[51] supone el primer texto europeo de regulación de la protección de datos como protección de la vida privada de la persona ante la informática. El convenio final contiene dos Resoluciones anteriores que constituyen los dos primeros textos internacionales que contienen directrices dirigidas a los Estados sobre cómo actuar en el ámbito de esta materia, por lo que tuvieron una clara influencia en las legislaciones en que se dictaron[52].

Consta de 27 artículos divididos en siete capítulos, participando de las decisiones previas del Consejo de Europa en la defensa de los derechos humanos. La finalidad del mismo es de armonización o coexistencia de dos derechos en liza: la protección de los datos de la persona con la libre circulación de la información.

El Convenio surgió como desarrollo del art. 8 del CEDH, con la finalidad de garantizar, a los ciudadanos de los Estados contratantes, el respeto de sus derechos y libertades, en

[49] Se dictaron en los casos "*Österreichischer Rundfunk*" y "*Lindqvist*". En ésta última, el TCE se pronuncia sobre "los datos relativos a la salud", que tendremos ocasión de ver en el capítulo II de este trabajo**.** SSTJCE, 20 de mayo de 2003, asunto C-465/00, y 6 de noviembre de 2003, asunto C-101/01; respectivamente.

[50] Se dictó con el doble objetivo de garantizar el derecho a la vida privada reconocido en el art. 8 CEDH, y en concreto en lo relativo a la protección de datos personales y el de impedir la restricción de la libre circulación de los datos personales, a través del reconocimiento de unos principios comunes para todos los Estados miembros.

[51] Constituye un desarrollo del art. 8.1 del Convenio de Roma para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Fue firmado por España el 28 de enero de 1982, ratificado el 27 de enero de 1984, y publicado el 15 de noviembre de 1985.

El Convenio n.º108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física "el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona" (http://www.europarl.europa.eu).

El Protocolo, aprobado por el Comité de Ministros de la UE, el 18 de mayo de 2018, ha modificado el Convenio (denominándose Convenio 108+), y con él se pretende ampliar su ámbito de aplicación, aumentar el nivel de protección de los datos y mejorar su eficacia.

[52] Resoluciones del Comité de Ministros del Consejo de Europa*:*

Resolución (73) 22, de 26 de septiembre de 1973, sobre la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado, y Resolución (74) 29, de 20 de septiembre de 1974, sobre la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público.

particular, derecho a la vida privada frente al tratamiento de los datos personales; garantizando unos principios generales básicos para todo el tratamiento de datos personales.

Así, el objetivo del Convenio era compatibilizar la garantía del derecho fundamental al respeto a la vida privada y el libro flujo de información entre los Estados miembros[53]; extendiendo su protección a cualquier tratamiento de datos, público o privado, de carácter automatizado, previendo que pudiera contemplar cualquier técnica de procesamiento (inclusive los no automatizados) y extenderse a datos de personas jurídicas o entes sin personalidad[54].

El Convenio trató de garantizar un estándar mínimo de protección, ampliable por las legislaciones nacionales, debido al incremento del flujo transfronterizo de datos personales sometidos a tratamiento automático, que ya en la época de los ochenta se vislumbraba[55]. El objeto de protección del convenio son los datos personales y el tratamiento de los mismos; considerando "dato personal" cualquier información relativa a una persona física identificada o identificable", a la que se denomina "persona concernida" (art. 2.a). Y si estos datos personales forman un conjunto y éste es objeto de tratamiento automatizado[56], estaremos ante un "fichero automatizado" (art. 2.b).

Su gran aportación fue otorgar carácter vinculante a los principios generales de la protección de datos establecidos en las Resoluciones (73) 22 y (74) 29, estableciendo un conjunto de principios básicos para la protección de datos y los criterios que regulan su tratamiento y flujo, creando además una Autoridad de Control[57].

Siguiendo con el Convenio, en relación con el contenido del derecho a la protección de datos, a diferencia de los clásicos derechos de prestación o de libertad, el derecho a la

[53] Según señala la Exposición de Motivos.
[54] *Ibid*., p. 29
[55] GUICHOT REINA, E., *Datos personales y Administración Pública*, Thompson-Civitas, Madrid, 2005, pp. 28 y ss.
[56] Habrá que entender por tratamiento automatizado, "cualquier operación consistente en el registro de datos, su aplicación a operaciones matemáticas, modificación, borrado, extracción o difusión; y se utilicen total o parcialmente procedimientos automatizados, debiendo entender comprendida la recogida de datos, al así preverse para entender leal un tratamiento de datos" (art. 2.c).
[57] LAZPITA GURTUBAN, M, "Análisis comparado de las legislaciones sobre protección de datos de los Estado miembros de la Comunidad Europea", Informática y Derecho, *Revista Iberoamericana de Informática y Derecho*, 1994, nº 6-7, p.405.

protección de datos personales está integrado por un conjunto de facultades relativas a la libre disposición sobre los propios datos personales; por un poder de control sobre ellos, sobre su uso y finalidad o destino. Estas facultades son las siguientes:

a) Derecho a ser informado. El titular de los datos debe ser informado de la utilización de sus datos y de su finalidad. No se recoge en la CDFUE[58] y si en la Directiva 95/46/CE.

b) Derecho a la libre disposición de los datos: el consentimiento. Derecho de autodeterminación previa información: consentimiento informado.

c) Derecho de acceso, oposición, rectificación y cancelación (derechos ARCO).

El de acceso junto el de rectificación son los únicos mencionados en la CDFUE (art. 8).

1.2.1.2. Principios relativos al tratamiento de datos personales, recogidos en la normativa del Consejo de Europa (Resoluciones y Convenio 108)

El Convenio se basa en lo que denomina la "calidad de los datos", constituida entorno a un conjunto de reglas o principios, que servirán posteriormente de inspiración a la legislación comunitaria y española, según veremos posteriormente.

1. Principios relativos a la calidad de los datos.

Sólo en el Convenio estos principios tienen carácter vinculante.

a) *Principio de lealtad*.

Los datos deben ser obtenidos y tratados de forma leal y lícita (art. 5.a). Este principio básicamente alude a las circunstancias de obtención de los datos, así como a la posibilidad que se le ofrece a su titular de saber los datos suyos que se han recogido y la facultad de ejercer los derechos ARCO[59].

b) *Principio de finalidad*.

[58] Carta Fundamental de los Derechos de la Unión Europea. 2000/ 364/01.
[59] ARENAS RAMIRO, *op.cit.*, pp. 168 y ss.

Para todo proceso de tratamiento de datos personales, los datos deben ser recogidos para unos fines legítimos y determinados, sin que puedan ser utilizados para otros fines incompatibles con éstos (arts. 5.1.b) y 15.1). Ello, debe llevarse a cabo antes de iniciarse el tratamiento de los datos, ya que sólo de esta forma puede comprobarse que se ajustan a la finalidad prevista.

c) *Principio de pertinencia*.

Los datos deben ser adecuados, pertinentes y no excesivos respecto de los fines para los que fueron recogidos (art. 5.c). Este principio se conecta con el de finalidad, ya que para valorar la pertinencia es necesario considerar si esos datos efectivamente cumplen con la finalidad prevista y se recogen sólo aquellos necesarios para la finalidad perseguida con el tratamiento.

d) *Principio de exactitud*.

Los datos recogidos y almacenados deben ser exactos y estar puestos al día (art. 5.d). en el momento de la recogida y en su transmisión debe comprobarse la exactitud y fiabilidad de los datos.

e) *Principio de conservación*.

Los datos deben conservarse de tal forma y durante un período de tiempo tal que sólo permita identificar a los titulares de los mismos durante el plazo estrictamente necesario para conseguir los fines para los que fueron recogidos (art. 5.e). Debe reconocerse el "derecho al olvido". Igualmente, este principio se conecta con el de finalidad, ya que deben conservarse mientras permanezca asociado a una finalidad, ya que, en caso contrario, deben destruirse, aunque puede conservarse si no se asocia a un titular concreto.

2. Principios relativos a la legitimación del tratamiento de datos.

El principal requisito es el consentimiento del titular, que constituye un auténtico derecho del titular de los datos, como facultad esencial del derecho a la protección de datos personales tratándose de la esencia del derecho a la libre disposición de los mismos[60]. El

[60] SÁNCHEZ BRAVO, A.A., *La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, Secretariado de Publicaciones, Sevilla, 1982, p. 82.

convenio no aborda de forma expresa la necesidad del consentimiento como parte del contenido necesario para el tratamiento de datos.

3. Categorías especiales de tratamiento de datos.

El Convenio se refiere a los datos especialmente sensibles, que deben recibir una especial protección. La regla general para ellos es la prohibición de tratamiento.

Se consideran datos sensibles, entre otros[61], aquellos que revelan el origen racial, las opiniones políticas, convicciones religiosas o de otro tipo, datos de salud o vida sexual y los relativos a condenas penales.

Estas normas que acabamos de ver suponen los primeros textos normativos europeos en los que se recogen los principios básicos de todo el tratamiento de datos personales, imponiendo pautas muy estrictas sobre los mismos para los Estados, y que siguen hoy vigentes, aunque adaptados a la actual época tecnológica.

1.2.1.3. Unión Europea

Desde principios de los años sesenta, se planteó la cuestión de la protección eficaz de los derechos fundamentales en el ordenamiento comunitario, siendo la posición inicial del TJCE el inhibirse al entender que no era su competencia. Así, esta llamada etapa "inhibicionista" derivó en que fueran los tribunales constitucionales nacionales los que se pronunciaran sobre estos casos[62]. No obstante, el propio TCJE corrigió este planteamiento comenzando gradualmente a reconocer competencia sobre la protección de los derechos fundamentales en el ordenamiento comunitario[63].

La segunda etapa de reconocimiento de los derechos fundamentales como principios generales del ordenamiento comunitario se sirve de la jurisprudencia del *Conseil D´Etat*

[61] No se trata de una lista cerrada, sino que cada Estado podrá ampliar esta lista, así como reducirla, aunque mediante ley en base a una finalidad legítima (arts. 9 y 11 Convenio).

[62] A esta situación se le conoció como "la rebelión de los tribunales constitucionales".

[63] A cerca de la cuestión de la evolución de la protección de los derechos fundamentales por el TJCE, entre otros autores, vid. CHUECA SANCHO, A.G., "La evolución de los derechos fundamentales en los tratados comunitarios", en MATIA PORTILLA, F.J., *La protección de los derechos fundamentales en la Unión Europea*, Civitas, Madrid, 2002, pp. 40-47.

francés, que la venía aplicando desde 1789, y es a través de la jurisprudencia del propio TJCE como se consolidan estos principios, para, posteriormente ser incorporados al derecho positivo. Así, el Tratado de Maastricht recoge en su art. 6[64] la obligación de respetar los derechos humanos y las libertades fundamentales, como principios generales del Derecho comunitario. De esta forma se ponen en conexión tres sistemas jurídicos distintos, resultado de la suma de los derechos contenidos en cada sistema: el de la UE, el del Consejo de Europa (mediante la remisión hecha al CEDH, y la jurisprudencia del TJCE, y el propio de cada Estado miembro[65].

El reconocimiento y garantía de los derechos fundamentales, tenía, por tanto, apoyo en el art. 6 Tratado de la Unión Europea (TUE)[66], además de lo previsto en el art. 46.d), por el cual se refuerza el papel del TJCE de garantía de los derechos fundamentales al extenderse a la actividad de las instituciones comunitarias. Sin embargo, se subrayó mediante un informe elaborado por un Grupo de Expertos[67] en derechos fundamentales la necesidad de que estos principios tuvieran un reconocimiento explícito, como vemos a continuación.

La tercera etapa de reconocimiento y garantía de los derechos fundamentales de la UE se inicia con la aprobación de la CDFUE, con el objetivo de traspasar el fuerte carácter económico de los Tratados que marcaban el mercado único, hacia una nueva vertiente política: la de los derechos de los ciudadanos.

De esta forma, la CDFUE vino a codificar los derechos fundamentales no escritos de la UE, conteniendo un reconocimiento expreso de derechos, de un sistema de "fuentes formales" de derechos, a partir de un sistema de "fuentes de inspiración", como señala

[64] Estas garantías son las que contiene el CEDH y siguen las tradiciones constitucionales de los países miembros de la UE. Art. 6:
"1. La Unión se basa en los principios de libertad, democracia, respeto de los derechos humanos y de las libertades fundamentales y el Estado de Derecho, principios que son comunes a los Estados miembros. 2. La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950, tal y como resultan de las tradiciones constitucionales comunes a los Estados miembros como principios generales del Derecho comunitario".

[65] ARENAS RAMIRO, *op.cit*., pp. 198 y ss.

[66] Tratado por el que se establece la Constitución Europea, firmado en Roma el 29 de octubre de 2004.

[67] Informe "*Afirmación de los Derechos fundamentales en la Unión Europea. Ha llegado el momento de actuar*", febrero de 1999, elaborado por un Grupo de Expertos, presidido por *Spiro Simitis*.

RUBIO LLORENTE[68]. Sin embargo, su eficacia vinculante quedó aplazada, entendiéndose que estamos ante un denominado "*soft law"*, desprovisto de fuerza vinculante, pero con una eficacia limitada o indirecta, al dotarse con un alcance jurídico interpretativo importante*;* lo que no impide reconocer la importancia de este texto.

La CDFUE reconoce en su art. 8 el derecho a la protección de datos personales como un derecho autónomo, separado y distinto del derecho al respeto a la vida privada y familiar, contenido en el art. 7[69]; con lo que se aparta del criterio seguido en el CEDH, en el Derecho comunitario y en la mayor parte de los Estados miembros[70].

El Tratado por el que se establece la Constitución Europea (TCE), vino a añadir, junto al art. 6 TUE, una nueva protección de los derechos fundamentales a través del art. I-9. De forma que, la CDFUE al estar integrada en la Parte II del Tratado se constituye en Derecho originario comunitario, garantizado por el TJCE, pasando el art. 8 de la CDFUE, en que se reconoce el derecho a la protección de datos personales; (dando, por tanto, CDFUE de naturaleza como derecho fundamental autónomo), a ser el artículo II-68 de dicho Tratado, en una redacción similar a la del art. 8 de la CDFUE.

El art. 5 TCE incorpora el principio de proporcionalidad, por el cual "(…) *ninguna acción de la Comunidad irá más allá de lo que es necesario para conseguir los objetivos*

---

[68] RUBIO LLORENTE, F., "Mostrar los derechos sin destruir la Unión", *Revista española de derecho constitucional*, Año nº 22, Nº 64, 2002, págs. 13-52

[69] "Artículo 7. Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
Artículo 8. "Protección de datos de carácter personal.
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."
Este planteamiento resulta muy moderno, y tiene en consideración los retos planteados por las nuevas tecnologías, como señala MARTÍN RETORTILLO, L, "Dos notas sobre la CDFUE", en ALONSO GARCÍA, R., Y GARCÍA DE ENTERRÍA (eds.), en *La Encrucijada constitucional de la Unión Europea*, Civitas, Madrid, 2002, p.192.

[70] Sobre los arts. 7 y 8 de la Carta, y otros preceptos, la bibliografía es muy abundante. Así, entre otros, destacamos:
RUIZ MIGUEL, C., "El derecho a la protección de datos personales en la Carta de Derechos de la Unión Europea: análisis crítico", en *Revista de Derecho Comunitario europeo*, año 7, nº 14, enero-abril 2003, pp. 7 y ss., RODOTÁ, Stefano, "Democracia y protección de datos", en *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre Protección de Datos, pp.15 y ss. Destacamos como este autor ha sido esencial en el reconocimiento del derecho a la protección de datos en la Carta. Igualmente, resulta fundamental su obra "*La vida y las reglas. Entre el derecho y el no derecho"*, Trotta, Madrid, 2010, pp. 69 y ss.
Para ver más información sobre la CDFUE, ver MANGAS MARTÍN, Araceli, "Carta de los derechos fundamentales de la Unión Europea. Comentario artículo por artículo", Fundación BBVA, 2008.

perseguidos por este Tratado". Este principio, como veremos más adelante, tendrá una gran importancia para valorar la licitud del tratamiento de datos personales.

Al mismo tiempo, el reconocimiento del derecho a la protección de datos personales se lleva a cabo en el art. I-51 TCE, con un contenido similar al del art. 286 TCE. Por ello, encontramos una doble configuración de la protección de datos en el TCE: en la Parte I y en la Parte II[71]. Por tanto, tomando como base, el artículo 16 del TFUE[72] y los artículos 7 y 8 de la CDFUE, la Unión debe garantizar la aplicación sistemática del derecho fundamental a la protección de datos, consagrados en la CDFUE[73] .

El art. 52 de la CDFUE establece los límites de los derechos fundamentales en la UE: Respeto al contenido esencial del derecho; previsión legal de la limitación; finalidad legítima de la limitación y proporcionalidad de la limitación.

1.2.1.4. Directiva sobre protección de datos en el ámbito penal

En mayo de 2018 también entró en vigor 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 para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

La Directiva protege el derecho fundamental de los ciudadanos a la protección de datos cuando los utilizan las autoridades encargadas de hacer cumplir la ley. Garantiza que los datos personales de víctimas, testigos y sospechosos de delitos sean debidamente protegidos, y facilita la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo.

[71] Se trata de una "repetición no deseada", en opinión de MARTÍNEZ MARTÍNEZ, R, *Una aproximación crítica a la autodeterminación informativa*, Thomson-Civitas, Madrid, 2004, pp. 220-221.
[72] Tratado de Funcionamiento de la Unión Europea. Firmado en Roma en 1957 como Tratado constitutivo de la Comunidad Económica Europea.
[73] https://www.europarl.europa.eu

1.2.1.5. Directiva sobre la privacidad y las comunicaciones electrónicas

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) fue modificada mediante la Directiva 2009/136/CE, de 25 de noviembre de 2009.

1.2.1.6. Reglamento relativo al tratamiento de los datos personales por las instituciones y organismos de la Unión

El 11 de diciembre de 2018 entró en vigor el Reglamento (UE) 2018/1725 del Parlamento Europeo y 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) n.º 45/2001 y la Decisión n.º 1247/2002/CE[74].

1.2.1.7. Otra normativa europea[75]

Hay otra normativa que tiene un amplio contenido en materia de protección de datos personales:

- El Sistema de Información Schengen (SIS), derivado del Convenio Schengen de 1990

- El Sistema de Información Aduanera (SIA)

- La Oficina Europea de Estadística (Eurostat)

- Sistema para la comparación de las impresiones dactilares (Eurodac)

[74] Esta información sobre las dos Directivas y el Reglamento han sido extraídas de la página web parlamento europeo (https://www.europarl.europa.eu)
[75] https://www.europarl.europa.eu.

- Sistema de información de Visados (VIS)

- Oficina Europea de Policía (Europol)

- Unidad de Cooperación judicial (Eurojust).

Además, el Consejo de Europa ha elaborado, además dos Convenios que guardan estrecha relación con la protección de datos personales: El Convenio sobre los Derechos Humanos y la Biomedicina de 1997 y el Convenio sobre el Cibercrimen de 2001.

En la actualidad se está examinando la nueva propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se derogaría la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas).

1.2.1.8. La protección de datos en la normativa y actos sectoriales

Además de los principales actos legislativos en materia de protección de datos antes señalados, también se establecen disposiciones específicas en esta materia en actos legislativos sectoriales, de las cuales resaltamos, por su importancia, las siguientes[76]:

- El artículo 13 de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave;
- El capítulo VI (sobre las garantías de protección de datos) del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol);

[76] Disponible en: https://www.europarl.europa.eu.

- El capítulo VIII (sobre protección de datos) del Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea.

1.2.2. LA LIBERTAD INFORMÁTICA Y EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

Como veíamos en el apartado anterior, hemos asistido a una evolución del derecho a la intimidad, en la que de partiendo de un reconocimiento inicial de reserva de aquello considerado como lo más personal e interno del ser humano, a ampliarse esta reserva del espacio de intimidad con un poder de disposición o control de su titular sobre todo aquello que forma su espacio más privado e íntimo en cuanto tiene repercusión externa.

Así, al mismo tiempo que se llevaba a cabo esta mutación, asistíamos a un fenómeno social con hondas influencias en muchos ámbitos de la sociedad. La revolución derivada de las nuevas tecnologías informáticas dio paso a la llamada Sociedad de la información y la comunicación, que vino a suponer un cambio radical de modelo de relaciones sociales, en el que, al mismo tiempo, empezaron a surgir temores por la influencia de la utilización de la informática, derivados de su afectación al ámbito privado e íntimo de las personas.

De esta forma, el impulso de la informática y las nuevas tecnologías de la época de aprobación constitucional venía a suponer una ayuda fundamental en el tratamiento de la información; pero, al mismo tiempo, implicaba el peligro de poder invadir esferas propias de la libertad de las personas. Por ello, la CE consciente de este peligro potencial que podría atentar contra la intimidad personal, viene a limitar la utilización de la informática como medio para garantizar el honor y la intimidad personal y familiar de los ciudadanos, así como el pleno ejercicio de sus derechos, junto al reconocimiento explícito del derecho al honor, a la intimidad personal y familiar, a la propia imagen y la protección de la inviolabilidad del domicilio y el secreto de las comunicaciones (art. 18.4). Por tanto, este precepto supone la respuesta constitucional a la libertad informática como "*una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona*".

Así, como mecanismo de defensa y protección de esta intimidad personal amenazada, surgieron dos instrumentos de tutela jurídica: la libertad informática y el derecho a la protección de datos personales; los cuales vendrían a coexistir y complementar al derecho a la intimidad.

Inicialmente el TC ha contemplado la informática como un medio técnico que pueden ocasionar injerencias en la intimidad de las personas, entendiendo la limitación del art. 18.4 CE como un derecho instrumental de la intimidad, que resulta necesario para protegerla frente a intromisiones externas[77]. Así, con la finalidad de regular el uso de la informática (limitación de la informática), la redacción del art. 18.4 CE se basó en el art. 8 del Convenio 108, así como en el artículo 12 de la Declaración Universal de Derechos Humanos[78] y el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos[79]. De esta forma, en el art. 18.4 CE se recoge, a través de la limitación de la informática, una nueva garantía constitucional, sin señalar cuales serían sus elementos esenciales, a diferencia de la detallada regulación de la pionera Constitución portuguesa de 1976.

Sin embargo, la evolución jurisprudencial ha venido acompasada a los cambios tecnológicos. Mientras la informática no estaba desarrollada, la intimidad mantenía un contenido definido. Sin embargo, ante la introducción de la informática esta concepción se ve impotente para dar protección a la intimidad ante la nueva realidad del almacenamiento de información personal, por lo que se reclamaba por parte de distintos sectores doctrinales una ampliación de la concepción inicial para adaptarla a las nuevas tecnologías, en el que se incluyera un derecho activo, de control sobre el flujo de informaciones que afectan a cada sujeto[80].

Así, el mayor riesgo de la utilización de la informática y de las nuevas tecnologías está en la posibilidad de invasión o intromisión de la vida privada ante la acumulación de cada vez más volumen de información; por ello, en cumplimiento del mandato constitucional del art. 18.4 CE se limita el uso de la informática y, por tanto, del tratamiento de datos,

[77] SERRANO PÉREZ, *op.cit.*, pp. 156 y ss.
[78] Declaración Universal de Derechos Humanos, ONU. Resolución 217 A (III), de 10 de diciembre de 1948.
[79] Pacto Internacional de Derechos Civiles y Políticos, ONU. Asamblea General, Resolución 2200 A (XXI), de 16 de diciembre de 1966.
[80] MARTÍNEZ DE PISÓN CAVERO, J.M., *El derecho a la intimidad en la jurisprudencia constitucional*, Civitas, Madrid, 1993, p. 64.

relacionándolo con el derecho a la intimidad. Notándose, como hace SUÁREZ RUBIO[81], que esto es muy interesante, debido a que esta protección también es garantía formal de la privacidad: así, este artículo sería una garantía para la plena efectividad de otros derechos, como el derecho a la intimidad.

Pese a la consagración constitucional de un nuevo derecho fundamental, la doctrina y la propia jurisprudencia no coinciden en cuanto a su denominación. Así, la denominación "derecho a la protección de datos", sin embargo, es compartida por otras denominaciones empleadas doctrinal y legalmente, como derecho a la intimidad y libertad informática (propias de una primera visión de la jurisprudencia constitucional) o derecho a la autodeterminación informativa (mencionado en las SSTC 254/93 y 290/2000).

Se denomina *Habeas Data*, a un aspecto más concreto referido a los derechos del interesado (inicialmente derechos ARCO, y luego ampliados: acceso, rectificación, supresión (derecho al Olvido), oposición, limitación del tratamiento, portabilidad y a no ser objeto de decisiones individualizadas), así como la principal garantía legal que tiene toda persona que facilita una información personal.

1.2.2.1. Reconocimiento constitucional

La doctrina del TC, hasta la STC 292/2000, ha sido contradictoria y confusa en cuanto a sus conclusiones. Así, en la STC 254/1993 se concibe la privacidad como una libertad positiva para ejercer un derecho de control sobre los datos de la propia persona que han salido de la esfera de la intimidad para convertirse en un archivo electrónico. Y es así, como en esta sentencia el Tribunal declara un derecho fundamental de libertad informática definiendo su contenido, del que luego se harán eco las SSTC 290/2000 y 292/2000. Y, refiriéndose al art. 18.4 CE, como garantía del derecho a la intimidad, señala:

> *"(…) De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último*

[81] SUÁREZ RUBIO, *op.cit*., pp. 5-9.

> *término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".*

Así, partiendo de la acuñación de la concepción de un nuevo derecho fundamental con un contenido propio y distinto del derecho a la intimidad, fundamental positivo y activo, frente al carácter negativo de este último, la primera ley española sobre protección de datos (LORTAD) reconocía esta diferencia entre intimidad y una nueva libertad (denominada privacidad, en la Exposición de Motivos), dotada de un contenido más amplio, más global de facetas de la personalidad del individuo.

Resulta fundamental resaltar la influencia de la sentencia de 15 de diciembre de 1993, del Tribunal Constitucional Federal Alemán[82], en la que por primera vez se acuña el derecho a la autodeterminación informativa como derecho de última generación, configurado así a partir del derecho a la personalidad garantizado en el art. 2 de la Ley fundamental de Bonn "(…) *la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la vida propia*".

A propósito de esta sentencia, señala GARRIGA GONZÁLEZ,[83] como del derecho al libre desarrollo de la personalidad el tribunal extrae la facultad de cada individuo de disponer de sus propios datos en cuanto a su revelación, y este poder de disposición o control de los datos propios es lo que constituye el derecho a la autodeterminación informativa, como derecho de la personalidad vinculado a la dignidad humana; el cual

[82] Esta sentencia declaraba inconstitucionales algunos preceptos de la Ley del Censo, de 31 de marzo de 1982, en concreto, planteaba una revelación muy amplia de los datos personales por los ciudadanos, bajo fuertes sanciones ante su incumplimiento.

[83] GARRIGA GONZÁLEZ, A., "El derecho a la autodeterminación informativa", en PÉREZ LUÑO, A., Problemas actuales de documentación y la información jurídica, Tecnos, Madrid, 1987, *op.cit,* pp. 29 y ss.

"*garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y utilización de sus datos personales".*

De esta forma, la autodeterminación informativa consistiría en la libertad para determinar quién, qué y con qué motivo pueden conocerse datos relativos a una persona. Por ello, estamos en presencia de un derecho fundamental que garantiza: "(…) *la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por él mismo cuando y dentro de qué limites procede revelar situaciones referentes a su propia vida*[84]".

Sin embargo, la cuestión más importante para el tribunal alemán es que "*la autodeterminación informativa no sólo depende de los datos sino de su elaboración*". No importa tanto si el dato, sea íntimo o no, sino que lo que importa es su utilidad y su posible aplicación: *"(…) las posibilidades que los mismos (los datos) tienen de elaboración e interrelación propias de la tecnología informática*", que pueden ser prácticamente ilimitadas. Por tanto, lo que justifica la protección de datos y, en definitiva, de la persona, no es su carácter en sí, sino el contexto en el que se usan[85].

Por ello, lo importante es la finalidad o propósito para la cual se recaban los datos, que procedimientos o posibilidades de interconexión y de utilización existen con los mismos y el uso o utilización que se dé a esta información. Sin embargo, la sentencia emitida por el tribunal alemán no atribuye a su titular un derecho absoluto e ilimitado sobre sus datos, sino que como cualquier derecho fundamental tiene limitaciones dirigidas a preservar los intereses generales[86].

Al mismo tiempo, como medio de defensa contra las intromisiones de la técnica informática que se producen en la vida privada de las personas, este derecho de autodeterminación debe dotarse de un elemento básico de defensa, que consiste en el

[84] SERRANO PÉREZ, *op.cit*., pp. 179 y ss.
[85] *Ibid*., p. 273.
Sobre la autodeterminación informativa, véase así mismo, PIÑAR MAÑAS, J.L., "Protección de datos: origen, situación actual y retos para el futuro", en PIÑAR MAÑAS, J.L., *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp.84 y ss.
[86] TRAVERSI, A., "*II Diritto dell, informática*", Seconda edizione, Ipsoa Informáticas, 1990, p. 92.

deber de información previa al titular de los datos sobre el contenido de los mismos, finalidad y utilización de su recogida y su cesión o no a terceros[87].

Sobre el derecho de autodeterminación informativa y su relación con el *Habeas Data*, se pronuncia MURILLO DE LA CUEVA, señalando que dicho *status* pretende satisfacer la necesidad de las personas de preservar su identidad controlando la revelación y el uso de los datos que les conciernen y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos propia de la informática, y de los peligros que esto supone. De forma que ese objetivo se consigue por medio de lo que se denomina técnica de protección de datos, "integrada por un conjunto de derechos subjetivos, deberes, procedimientos, instituciones y reglas objetivas*"*[88].

1.2.3. RECONOCIMIENTO DEL DERECHO A LA PROTECCIÓN DE DATOS: DOCTRINA CONSTITUCIONAL

El derecho a la protección de datos constituye un derecho autónomo e independiente de otros derechos; siendo instituto de garantía, además del derecho a la intimidad, de otros derechos fundamentales, como el libre desarrollo de la personalidad, a la igualdad, libertad sindical y no discriminación, libertad ideológica y religiosa, etc. Sin embargo, en el ámbito sanitario, como luego veremos en el capítulo II, habida cuenta de que los datos sanitarios se consideran datos sensibles y por tanto íntimos, los derechos fundamentales implicados en el ámbito sanitario serían el derecho a la intimidad y el derecho al control de los datos personales[89].

Como hemos visto, nuestra Constitución junto a la portuguesa fueron las primeras en abordar las relaciones entre la informática y los derechos fundamentales, mediante un precepto (art. 18.4) del que se traduce una posición "defensiva" frente a la informática, en el que no se tienen en cuenta otras vertientes de las relaciones entre informática y

[87] HERRANZ ORTÍZ, I., *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, *1999,* pp. 85 y ss.

[88] MURILLO DE LA CUEVA, L., P., "El derecho a la autodeterminación informativa y la protección de datos personales", *Azpilcueta. Cuadernos de Derecho* (20), San Sebastián, 2008, pp. 43-58.

[89] El mayor número de reclamaciones y denuncias en materia de protección de datos se lleva a cabo en el ámbito de la salud, porque precisamente el ciudadano entiende que afectan a su ámbito más reservado, la intimidad. TRONCOSO REIGADA, A., *La protección de datos personales, en busca del equilibrio,* Tirant Lo Blanc, Valencia, 2010, pp. 64 y ss.

derecho; y que, a la vez, contiene una aparente contradicción, al referirse, de una parte, de forma expresa a los derechos a la intimidad y al honor, y de otra, al establecer una garantía instrumental del pleno ejercicio de (todos) los derechos, sin que se concrete que se trate de derechos fundamentales[90].

Del mismo modo, ante la ausencia inicial del reconocimiento constitucional concreto en los países firmantes del CEDH, han sido los tribunales constitucionales los que han venido interpretando como la protección de datos personales quedaba incluida en el derecho a la vida privada o dentro de otro derecho fundamental. De forma, que la jurisprudencia del TEDH ha tenido un papel decisivo en el reconocimiento y garantía del derecho a la protección de datos personales mediante la creación de un estándar mínimo sobre esta materia; considerando que los datos personales forman parte de la esfera privada y, por tanto, del ámbito protegido del derecho a la vida reconocido en el art. 8 CEDH[91].

Este nuevo derecho fundamental a la protección de datos también se configura, y se denomina así por distintos autores, como derecho a la autodeterminación informativa; según fue reconocido por el Tribunal constitucional alemán en la famosa sentencia de sobre la Ley del Censo de Población, en la que configura este derecho como la libertad del ciudadano para determinar libremente los aspectos que le permitan conocer la utilización de sus datos personales.

En cuanto a la definición de dato personal, las distintas regulaciones sobre la materia lo resumen como "cualquier información relativa a una persona física identificada o identificable". Sin embargo, como señala PIÑAR MAÑAS[92], pese a esa aparente uniformidad, esta definición resulta demasiado amplia e imprecisa; siendo compartida

[90] GUICHOT REINA, "Datos personales y Administración Pública", *op.cit*., pp.61 y ss.
[91] ARENAS RAMIRO, *op.cit*., pp.79 y ss.
[92] PIÑAR MAÑAS, J.L., "Concepto de dato personal", en TRONCOSO REIGADA, A., *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (Coord.), Civitas, Madrid, 2010, p.193.

esta indefinición por el Grupo de Trabajo GT29[93], al señalar que "refleja la intención del legislador europeo de mantener un concepto amplio de datos personales[94]".

Por su parte, el TC y la LOPD lo identifican con cualquier dato relativo a una persona, aunque considerando que a través del tratamiento automatizado puede llegar a conocerse aspectos privados de la persona. Sin embargo, el TS[95] ha entendido que se trata de datos relativos a la vida privada de las personas, distinguiendo entre datos de persona identificada o identificable, pero que no son personales, de los datos personales y datos íntimos. Veremos en el capítulo II, su configuración específica en el RGPD y la LOPDGG.

Sobre este derecho se pronuncian MURILLO DE LA CUEVA y PIÑAR MAÑAS, señalando que: *"...* Se ha convertido en una categoría transversal. Su carácter instrumental ha hecho que, a la postre, se cumpla el artículo 18.4 CE en la medida en que se preocupa por garantizar a los ciudadanos el pleno ejercicio de sus derechos, de todos sus derechos y no sólo de los previstos en su apartado primero*"*[96].

Así, para determinar el alcance de cualquier derecho, es necesario preguntarse para qué sirve el mismo, o sea que bien jurídico es el que protege y que facultades otorga al titular del derecho para defender eses derecho; de forma que, *"este derecho sirve para poner en manos de cada uno de nosotros los instrumentos para definir qué aspectos de nuestra vida deseamos -o no nos importa en determinadas ocasiones- que manejen otros. Es decir, para controlar el acceso a nuestros datos personales, a las informaciones de*

[93] Grupo de trabajo del artículo 29, Dictamen 4/2007.
El Grupo de Trabajo del Artículo 29, fue creado en 1996, siguiendo lo dispuesto en el artículo 29 de la Directiva 95/46/CE, con una finalidad consultiva e interpretativa. En el mismo se integran representantes de las autoridades nacionales de control de la protección de datos (ACPD) de cada Estado miembro, además del Supervisor Europeo de Protección de Datos (SEPD) y la Comisión Europea. Sus funciones, en virtud de lo dispuesto en la Directiva, consisten en la emisión de dictámenes sobre el nivel de protección en la UE y terceros países, asesorar a la Comisión sobre proyectos normativos y formular recomendaciones (emite además, informes, dictámenes, y Documentos de trabajo). Sus decisiones no son vinculantes, pero tienen un valor doctrinal importante, y a ellas acuden con frecuencia tanto legisladores como operadores judiciales tanto europeos como nacionales. Accesible en: http://ec.europa.eu/justice/data-protection/index es.htm.

[94] PIÑAR MAÑAS, J.L., "Comentarios al artículo 3 de la LOPD", en TRONCOSO REIGADA, A. (Dir.), "Comentario a la Ley Orgánica de protección de datos de carácter personal", Civitas, pp. 193-194.
APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de protección de datos de carácter personal*, Pamplona, Aranzadi, pp. 58-64.

[95] STS de 11 de marzo de 2000.

[96] MURILLO DE LA CUEVA, P.L., y PIÑAR MAÑAS, J.L., "El derecho a la autodeterminación informativa", *Fundación Coloquio Jurídico Europeo*, Madrid, 2009, pp. 70-72.

cualquier tipo que nos identifiquen directa o indirectamente, y su uso por terceros, ya sean estos sujetos públicos o privados'[97].

Podemos decir, con PIÑAR MAÑAS, que el RGPD, al igual que el TJUE, no definen el derecho a la protección de datos, señalando, en línea con la STC 290/2000, que debe entenderse que el mismo "atribuye a una persona física el poder de disposición sobre sus propios datos, sean íntimos o no, siempre que estén o vayan a estar sometidos a un tratamiento, informatizado o no"[98]. Por tanto, "las personas físicas deben tener el control de sus propios datos personales" (Considerando 7 del RGPD); de forma que, como señala LESMES SERRANO[99], es ese control el que constituye el elemento central de este derecho, el que justifica sus principios[100] y el reconocimiento de los derechos de los titulares de datos afectados[101].

Para hacer efectivo el cumplimiento del derecho a la protección de datos, debemos tener en cuenta que el control de éste se basa en dos elementos fundamentales:

a) por un lado, el consentimiento del afectado para el tratamiento de sus datos por terceros. Así, este consentimiento deberá ser libre e informado, de modo que otorgue certeza a ambas partes sobre el conocimiento efectivo sobre qué es lo que se está autorizando; b) no obstante, existen ocasiones en que estos datos pueden ser manejados sin la previa autorización del titular de éstos. Para que esto se pueda realizar de forma lícita, es necesaria una Ley que lo autorice ya sea en forma genérica o específica. Y este sería el segundo elemento, la autorización legal para el tratamiento de determinados datos. En resumen, el consentimiento y habilitación legal son los títulos que autorizan el tratamiento de datos personales.

Junto a los dos elementos señalados en el apartado anterior, el propio art. 6 RGPD contempla otros, tales como que el tratamiento sea necesario en la ejecución de un

---

[97] *Ibid*., pp. 60-63.
[98] PIÑAR MAÑAS, J.L. "Objeto del Reglamento", en *Reglamento General de Protección de Datos*…, p. 57.
[99] LESMES SERRANO, C., "Comentario al artículo 1", en LESMES SERRANO, C (Coordinador), *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008, pp. 48 y ss.
Véase además, PIÑAR MAÑAS, J.L., "Derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", Asamblea: Revista Parlamentaria de la Asamblea de Madrid, nº 13, 2005, pp. 21-46.
[100] Arts. 5 a 11 del RGPD.
[101] Arts. 12 a 23 del RGPD.

contrato, en la protección de intereses vitales del interesado u otra persona, en el cumplimiento de una misión pública, o para satisfacer intereses legítimos del responsable del tratamiento.

Cabe destacar que la existencia de uno de estos dos supuestos no significa que el titular pierda su capacidad de autodeterminación, sino por el contrario, dispone de una serie de derechos sobre la disposición y control de sus datos, comenzando por el derecho a revocar la autorización cuando existiera. Además, el titular cuenta con una serie de facultades que tienen por objeto permitir el ejercicio de su poder de consentir el tratamiento de sus datos y reaccionar, en caso de ser necesario contra quienes hagan un uso indebido de los mismos.

Este derecho, está compuesto como dijimos por una serie de fundamentos o derechos derivados destinados a hacer efectivo el cumplimiento del derecho principal. Estos fundamentos o derecho podemos enumerarlos de la siguiente manera:

a) Derecho a ser informado cuando se recogen los datos.

b) Derecho a conocer el fichero y el tratamiento que tendrán sus datos personales.

c) Derecho a acceder a los datos de modo de conocer que información personal se encuentra en ellos.

d) Derecho a rectificar los datos que no sean correctos o exactos.

e) Derecho al Olvido, sobre los datos que ya no quiera que sean trataros o hayan perdido la calidad que tenían al memento de ser recabados.

f) Derecho de oposición sobre el tratamiento de determinados datos.

g) Derecho al resarcimiento de los daños causados a causa del tratamiento de los datos de modo ilícito.

h) Derecho a ser protegido por las Instituciones creadas para este propósito.[102]

[102] MURILLO DE LA CUEVA, P.L. "Informática y protección de datos personales (estudios sobre la Ley Orgánica 5/1992, de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal)", *Cuadernos y Debates*, *Centro de Estudios Constitucionales*, Madrid, 1993, pp. 60-65.

A estos derechos iniciales habría que añadirles las facultades actualizadas incluidas en los arts. 15 a 22 del RGPD, como las derivadas del derecho de cancelación, limitación del tratamiento, derecho de oposición y de decisiones individuales automatizadas, derecho a la portabilidad.

A los anteriores derechos, hay que sumarle una serie de principios que fueron aprobados en la *Declaración de Montreux*, entre los que se destacan:[103]

- Principio de recogida y proceso legítimo de los datos.
- Principio de calidad.
- Principio de finalidad y limitación.
- Principio de proporcionalidad.
- Principio de transparencia.
- Principio de participación individual y en particular, garantía de derecho de acceso de los interesados.
- Principio de no discriminación.
- Principio de seguridad de los datos.
- Principio de responsabilidad.
- Principio de supervisión independiente y sanción legal.
- Principio de nivel adecuado de protección en caso de movimientos transfronterizos de datos personales.

Partiendo de la consolidación de estos principios en la normativa del Consejo de Europa (Convenio 108 y Resoluciones) el RGPD mantiene la vigencia de los principios

[103] XXVII Conferencia Internacional de Autoridades de Protección de Datos, Montreux, Suiza, septiembre 2005, sobre "La protección de los datos personales y la privacidad en un mundo globalizado". Disponible en: https://apdcat.gencat.cat/es/documentacio/jornades_i_congressos/internacionals/

conocidos en materia de protección de datos, aunque, como veremos, ha añadido, siendo estos principios el fundamento de este derecho. Son de destacar, por su relevancia, los siguientes principios:

- *Prohibición salvo autorización*: este principio, prohíbe de antemano el procesamiento de datos que no hayan sido permitido previamente, ya sea por el consentimiento expreso del titular o por autorización legal. Este precepto ha generado gran controversia, puesto que, con el Reglamento Europeo, este principio se aplica indiscriminadamente a cualquier tipo de datos personales, siendo que no todos los datos tienen la misma trascendencia.
- *Limitación de la finalidad*: la recopilación de los datos, debe darse bajo objetivos específicos, y no podrán usarse para ningún fin distinto para el que fueron recabados. El Reglamento exige que para recoger los datos se deberá establecer previamente los fines para los que se obtienen los datos y deberá documentarse el uso futuro de los mismos. Cuando un dato recabado con cierta finalidad quiere usarse para otra distinta, es necesaria la justificación por separado y autorización expresa, aunque las modificaciones posteriores de los objetivos están limitadas a determinadas circunstancias y bajo una justificación fundada.
- *Minimización de datos*: este principio exige que las empresas recopilen la menor cantidad de datos posible. Por tanto, limita la recopilación al objetivo específico imprescindible para los que fueron recabados, prohibiendo a las empresas la recopilación desmedida de datos.
- *Transparencia*: este principio implica el conocimiento de los interesados sobre el tratamiento de los datos de manera comprensible. Las empresas deberán aclarar bajo petición cuales datos obtuvo y como serán utilizados.
- *Confidencialidad*: quienes recaban y procesan datos, tienen la obligación de protegerlos de forma técnica y organizativa, tanto en lo que refiere a su tratamiento como modificación sin autorización, así como del robo o destrucción de estos. La mayor novedad al respecto es la obligación explícita para aplicar medidas técnicas de protección. No obstante, estas medidas no se encuentran desarrolladas en el Reglamento de forma precisa, por lo que gozan de un margen interpretativo.

1.2.3.1. Doctrina constitucional

La libertad informática tuvo su reconocimiento constitucional con la STC 254/93, al establecer que el art. 18.4 CE, como garantía del derecho a la intimidad: *"(...) ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona (...)"*.

Y esta llamada "libertad informática" es "(…) *el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención" (*SSTC 11/1998, FJ 5, 94/1998, FJ 4*). A*sí, esta proclamada, libertad informática tendría por objeto el tratamiento automatizado de datos, en línea con lo que propugnaban el Convenio 108 y la LORTAD.

El TC se pronuncia por primera vez sobre el alcance de la autodeterminación informativa en la sentencia 254/1993, de 20 de julio[104], sentando las bases de lo que constituye el concepto y contenido esencial de este derecho, señalando que el art. 18.4 CE consagra un nuevo derecho fundamental autónomo y distinto del derecho a la intimidad, a la vez que instrumental para garantizar la efectividad de otros derechos fundamentales[105]; señalando, al mismo tiempo, que se trata de:

> "(…) *una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona*

[104] El TC en esta y posteriores sentencias utiliza la denominación de "libertad informática", posteriormente en las SSTC 290 y 292, ambos de 2000, se refiere al "derecho a la protección de datos personales", y también a la "autodeterminación informativa", en la última citada.

[105] Esta configuración general sólo se excepciona en la STC 143/1999, de 9 de mayo, que asimila el derecho a la intimidad con el de autodeterminación informativa.

> *provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática*".

Sin embargo, este planteamiento llegó a empañarse en posteriores argumentaciones vertidas en distintas sentencias, dando lugar a cierta ambigüedad, al identificar protección de datos con el derecho a la intimidad, el cual integraría dentro de su contenido la facultad de acceder a los propios datos, como se puso de manifiesto por la doctrina[106].

Le siguieron otro grupo de sentencias[107], en las que se señala como el art. 18.4 CE viene a suponer un "*derecho instrumental ordenador a la protección de otros derechos fundamentales*", en el cual se "*consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona pertenezcan o no al ámbito más estricto de la intimidad*"; diferenciando entre privacidad (que tendría un contenido más amplio) e intimidad. De esta forma, el fundamento del derecho a la protección de datos estaría en evitar discriminaciones.

La consideración dual del derecho a la protección de datos, como derecho autónomo, dirigido a la protección frente a las intromisiones ilegítimas, y como derecho instrumental, que sirve para garantizar básicamente el derecho al honor y a la intimidad, se manifiesta igualmente en la STC 202/1999, de 8 de noviembre, en la que se cuestionaba el tratamiento de un fichero privado de bajas de enfermedad (nominativo) sin consentimiento expreso de los afectados; considerando que en el fichero sólo figuran las altas y bajas médicas, por lo que, entiende, que su finalidad no es médica sino de control del absentismo laboral. Por ello, al no existir consentimiento del afectado, el Tribunal entiende que existe desconexión entre la información personal recabada y el objetivo legítimo para la que fue solicitada, concediendo el amparo solicitado.

Sin embargo, la constitucionalización del derecho a la protección de datos como derecho fundamental surge a raíz de la resolución de los recursos de inconstitucionalidad presentados contra la LORTAD (STC 290/2000, de 30 de noviembre) y la LOPD (STC 292/2000, de 30 de noviembre). Así, el TC, se hace eco del planteamiento contenido tanto

[106] GONZÁLEZ MURÚA, A.R., "Comentario a la STC 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales", *Revista Vasca de Administración Pública*, nº 37, 1993, pp. 227-270.

[107] Dictadas entre 1998 y 1999, entre ellas la nº 11/1998, de 13 de enero, relativas al supuesto uso indebido por parte de la empresa Renfe de ficheros de trabajadores que incluían información sindical.

en la LOPD como en la Directiva 95/46/CE, estableciendo la configuración de un nuevo derecho fundamental que extiende su ámbito de aplicación a cualquier tipo de tratamiento de datos, ya sean informatizados o no; y en el que los derechos protegidos trascienden más allá del derecho a la intimidad, para abarcar a todos los derechos fundamentales.

En la STC 290/2000, se señala que el art. 18.4 hace referencia a una "(…) *garantía concreta (la ley que regule el uso de la informática) al servicio de un derecho que no aparece mencionado, el derecho a la protección de datos personales, derecho fundamental autónomo a la vez que instrumental para la efectividad del resto de los derechos"*. De ahí que habría que considerar el bien jurídico protegido, que no es otro que la protección de datos[108].

"El derecho a la libertad informática o autodeterminación informativa constituye el contenido esencial del art. 18.4. CE", al proclamar la STC 292/2000, de 30 de noviembre, que el derecho a la protección de datos se manifiesta de las siguientes formas*:*

Así, la libertad informática o derecho a la protección de datos personales es el derecho a controlar la información personal informatizada, con el objeto de garantizar la libertad de las personas frente a los riesgos de derivados de los bancos de datos. La posibilidad de su titular de poder decidir sobre sus datos personales se recoge en la STC 292/2000, al señalar cual es el contenido del derecho fundamental a la protección de datos:

> " *(…) 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*

[108] "La LORTAD, en efecto, ha sido dictada en cumplimiento del mandato contenido en el art. 18.4 CE de limitar el uso de la informática para garantizar ciertos derechos fundamentales y el pleno ejercicio de los derechos de los ciudadanos, de manera que si se considera la actividad aquí examinada como meramente instrumental o accesoria de otras materias competenciales, es claro que con este planteamiento se está desvirtuando cuál es el bien jurídico constitucionalmente relevante, que no es otro que la protección de los datos de carácter personal frente a un tratamiento informático que pueda lesionar ciertos derechos fundamentales de los ciudadanos o afectar al pleno ejercicio de sus derechos, como claramente se desprende del tenor de dicho precepto constitucional. Lo que guarda entera correspondencia, además, con el objeto de dicha Ley, que no es otro, según se ha dicho, que el de establecer un régimen legal para "limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de datos de carácter personal" que permita garantizar el respeto o el pleno ejercicio de tales derechos (art. 1). A lo que cabe agregar que la LORTAD también es la Ley que ha desarrollado un derecho fundamental específico, el derecho a la protección de los datos personales frente al uso de la informática, como antes se ha expuesto" STC 290/2000 (FJ 11).

> *también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso*"(FJ 7).

Por ello, estos poderes de disposición y control deben proyectarse en una serie de principios y derechos que se concretan jurídicamente su ejercicio:

> *"(…) 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 o usos posibles, por un tercero, sea el Estado o un particular".*

Al mismo tiempo, este derecho fundamental atribuye a su titular un conjunto de facultades:

> *"(…) consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos" (FJ 6).*

Como una parte fundamental del contenido esencial de este derecho resalta la necesidad de prestar consentimiento sobre las distintas operaciones a las que pueden someterse los datos personales. Como veremos en el capítulo III, para la jurisprudencia (STC 292/2000) y la doctrina científica[109], el consentimiento es el armazón sobre el que se construye el sistema de protección de datos personales para hacer frente a los usos de la informática, el otro pilar lo constituye el conjunto de derechos a disposición del interesado –*habeas*

[109] Como tendremos ocasión de ver seguidamente en el capítulo II.

data- que hacen que pueda llevarse a cabo dicha protección. De esta forma, junto al poder de disposición y control por parte de su titular, el contenido esencial del derecho a la protección de datos lo constituye un conjunto de derechos de su titular que garantiza un ámbito de protección en la utilización de los datos personales, que, a modo de límite de ejercicio del derecho, deben ser respetados en cualquier regulación: los llamados inicialmente derechos ARCO, ampliados posteriormente a raíz del RPGDD y la LOGPDP.

Sin embargo, el derecho a la protección de datos sus límites, al igual que sucede con todos los derechos fundamentales, en los que existen limitaciones[110], no tiene carácter absoluto, debiendo ceder cuando es necesario preservar otro derecho, un interés general o un bien constitucionalmente protegido, en la línea de lo marcado por el TC en la STS 292/2000. Así, la imposición de límites al derecho a la protección de datos debe cumplir los siguientes presupuestos:

a) Han de tener un fundamento constitucional, encontrándose las limitaciones en los demás derechos fundamentales y bienes jurídicos constitucionales (en concreto, el derecho de acceso al art. 105.b) CE y el derecho a la intimidad del art. 18.1 CE);

b) Han de estar previstos en la Ley, ser proporcionados y contar con la suficiente concreción;

c) La Ley que limite el contenido del derecho debe respetar, en todo caso, su contenido esencial, que para el derecho a la protección de datos se manifiesta en la garantía de protección de los derechos del titular de los datos.

Estas limitaciones se identifican con los derechos de información y ARCO, como señala la STC 292/2000 (FJ 11),

> *"(...) el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues*

[110] Como se pone de manifiesto, entre otras, en la STC 2/82 de 29 de enero.

> *así lo exige el principio de unidad de la Constitución. Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. (FJ 11)".*

En este mismo sentido, se pronuncia la STC 39/2016[111], señalando que:

> *"(…) el derecho a la protección de datos (art. 18.4 CE) no es ilimitado y puede encontrar condicionantes en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos".*

Por tanto, será la ley a la que corresponde establecer los límites del derecho fundamental junto con el desarrollo del mismo, para lo que habrá de tener en consideración el contenido esencial del derecho a restringir[112]; sin que, en ningún caso, la limitación pueda hacer impracticable el derecho o ineficaz la garantía concedida.

1.2.3.2. Reconocimiento legal

La Ley que desarrollara el art.18.4 CE debería, de una parte, regular la informática, imponiendo deberes a los titulares de los ficheros (cuando regula el tratamiento o la

[111] STC 39/2016, de 3 de marzo.
Esta sentencia se produjo en el juicio sobre los límites del derecho de un trabajador despedido por incurrir en falta grave, se cuestiona la admisión como prueba de un video que la empresa tomó a través de cámaras de seguridad y colocó sin aviso previo al personal, en función de proteger su patrimonio y no, supuestamente, para monitorizar el trabajo de la recurrente, medida que la demandada consideró justificada, idónea, necesaria y equilibrada, en vista que no se produjo vulneración alguna del derecho a la intimidad personal ni a la protección de datos de la trabajadora. Los argumentos en contra de la decisión del Tribunal Constitucional, plasmados en los votos particulares de algunos magistrados, confirman la concienciación actual de la sociedad y la interpretación acorde a los tratados internacionales adoptados por la legislación española, necesaria para reconocer el derecho y aplicar la sanción.

[112] SSTC 57/1994, de 28 de febrero y 18/1999, de 22 de febrero.

creación, modificación y supresión de ficheros), imponiendo deberes a los titulares de los ficheros; y de otra, abordar la regulación del derecho a la protección de datos (cuando establece los derechos de información y los derechos ARCO)[113].

Así, el desarrollo legislativo del art. 18.4 CE se ha producido a través de la LORTAD y la LOPD; la cual, respetando el núcleo duro de la LORTAD, se limitó a adaptarlo a las diferencias con la Directiva 95/46/CE, a la vez que se introducían algunas modificaciones[114]; siendo su objeto " (…) *garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*"[115]. De esta forma, resalta su carácter instrumental para la protección de los derechos fundamentales de las personas, aplicándose al tratamiento –automatizado o no- de los datos personales.

Tanto la LORTAD y la LOPD, ya desplazadas del ordenamiento jurídico, primero por el RGPD como, posteriormente, por la LOPDGDD, han servido para la elaboración de lo que constituye Derecho comparado; constituyendo, por tanto, aportaciones esenciales en el desarrollo y construcción del derecho fundamental a la protección de datos de carácter personal, conforme a los arts. 18.4 y 81.1. CE.

Considerándose que el art. 2.3 LOPDGDD declara la supletoriedad del RGPD y de la LOPDGDD, a falta de legislación específica, también para los tratamientos a los que el Reglamento General no resulte directamente aplicable por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea.

En este sentido, no olvidemos la trascendencia del RGPD, como derecho directamente aplicable a los Estados miembros que, como señala PIÑAR MAÑAS "pretende armonizar el derecho a la protección de datos en la UE, y se aplicará a empresas de todos los sectores económicos, no sólo europeas, sino también, en determinadas circunstancias, de fuera de la UE*"*[116].

[113] GUICHOT REINA, E., "Datos personales y Administración Pública", *Op.cit*., pp. 74 y ss.
[114] Básicamente, la creación del censo promocional y previsiones respecto de la utilización de datos para tareas de marketing directo.
[115] Art. 1 LOPD.
[116] PIÑAR MAÑAS, J.L., *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad*, Introducción, Reus Ediciones, PIÑAR MAÑAS (Dir.), Madrid, 2016.

2. GARANTÍAS DEL SISTEMA

2.1. AUTORIDADES DE CONTROL INDEPENDIENTES

2.1.1. NECESIDAD Y TRASCENDENCIA DE LAS GARANTÍAS FRENTE A LA INVASIÓN DE LA PRIVACIDAD

En correspondencia con la propia evolución del reconocimiento del propio derecho a la protección de datos, su garantía constitucional ha pasado de los inicios vacilantes a una institucionalización más segura con las STC 254/1993[117] y STC 202/1999[118]; las cuales proclaman la necesidad de garantías adecuadas; ya que:

> *"(...) un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta"*[119].

La STC 76/2019[120] remite a la STC 292/2000 para la necesidad de establecer las garantías adecuadas para procurar el respeto del contenido esencial del derecho fundamental a la protección de datos personales; pudiendo, de ello, extraerse las siguientes conclusiones:

Sobre la materia de protección de datos en el ámbito legislativo, vide "PIÑAR MAÑAS, J.L., *Código de Protección de Datos*, La Ley, Madrid, 2019. Para una primera aproximación al Reglamento desde la visión del modelo anglosajón, ver PIÑAR MAÑAS, J.L., "Reglamento Europeo de Protección de Datos: retos y oportunidades para la abogacía", Revista del Consejo General de la Abogacía Española, nº 98, 2016, pp.26-29.

[117] STC 254/93, de 20 de julio, "El mandato legislador que contiene el art. 18.4 C.E. requiere una intervención legislativa, que mientras no se produzca hará que falte la organización y los procedimientos necesarios para asegurar la protección de los datos personales. Ello no quiere decir que se carezca en el Derecho español de toda garantía constitucional en esta materia, sino que esa garantía se refiere al mínimo esencial, que opera mejor como defensa o razón jurídica para resistir una injerencia que como título para imponer deberes de prestación a los poderes públicos: así la negativa de un ciudadano, en determinados casos, a suministrar datos relativos a su origen racial o a su vida sexual, pero difícilmente se pueden garantizar prestaciones informativas sin crear la apropiada organización "(FJ 8).

[118] STC 202/1999, de 8 de noviembre.

[119] STC 143/1994, FJ 7, de 9 de mayo. En el mismo sentido, STC 94/1998, de 4 de mayo, FJ 4.

[120] STC 76/2019. La cual define el régimen jurídico vigente de tratamiento de datos personales, en base a la relación entre el RGPD y la LOPDGDD, y que veremos en el capítulo II.

- La previsión legal y la legitimidad del fin perseguido son requisitos necesarios, pero no suficientes para fundamentar la validez constitucional de una regulación del tratamiento de datos personales, pues para ello se requieren también "garantías adecuadas frente al uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento informático".
- Esas garantías son necesarias "para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos" y "para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos".
- La mera inexistencia de "garantías adecuadas" o de las "mínimas exigibles a la Ley" constituye de por sí una injerencia en el derecho fundamental, de gravedad similar a la que causarían intromisiones directas en su contenido nuclear.
- La exigencia de "garantías adecuadas" se fundamenta, por tanto, en el respeto del contenido esencial del derecho fundamental.

El Tribunal deduce del fallo que las "*garantías adecuadas" o "garantías mínimas exigibles a una Ley sometida al insoslayable respeto al contenido esencial del derecho fundamental cuyo ejercicio regula*", deben diferenciarse también del "*haz de facultades que componen el contenido del derecho fundamental a la protección de datos de carácter personal*", que, como se indicó antes, son aquellas que otorgan al titular del derecho fundamental "*un poder de disposición y de control sobre los datos personale*s".

Si el derecho fundamental a la protección de datos se puede asumir como un derecho a disponer de “garantías adecuadas”, cuando el tratamiento afecta a categorías especiales de datos, también llamados datos sensibles -pues el uso de estos últimos es susceptible de comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad- estas garantías no se encuentran delimitadas en la legislación, y el titular del derecho está igualmente desamparado, por lo que el Tribunal declara la inconstitucionalidad de la norma aplicable a los procesos electorales y también de la disposición final tercera, apartado dos, de la LOPDGDD.

2.1.1.1. Medidas provisionales y de garantía de los derechos en materia de protección de datos

El derecho a la tutela judicial efectiva (art. 24 CE) constituye uno de los pilares básicos del Estado de Derecho, manifestada en el derecho que toda persona tiene de acudir libremente a la justicia en defensa de sus derechos e intereses, garantizándose la no indefensión y a la utilización de un sistema de recursos, mediante las garantías procesales necesarias para que el proceso sea eficaz y sin dilaciones indebidas; que trasladado al ámbito material de los datos personales, supone que, en el ejercicio del derecho de defensa ante la vulneración de los derechos reconocidos en el RGPD, cualquier interesado que entienda vulnerados sus derechos en el tratamiento de datos personales podrá presentar una reclamación ante la autoridad de control; la cual tomará una decisión, pudiendo imponer la obligación de indemnizar al afectado (art. 82.4 RGPD) por parte del responsable o encargado del tratamiento (art. 77 RGPD). Como señala RECIO GAYO, el derecho a la tutela judicial efectiva ha pasado de ser un "complementario" (según la propuesta modificada de la Directiva de 1990) a un derecho fundamental incorporado en el art. 47 de la CDFUE y desarrollado, en lo relativo al derecho fundamental a la protección de datos en el RGPD[121]

A diferencia del RGPD, la LOPDGDD sí detalla los procedimientos a seguir de forma interna por las autoridades de control, dedicando el Título VIII a los procedimientos tramitados por la AEPD, en el caso de posible vulneración de la normativa sobre protección de datos (a ellos nos hemos referido detalladamente, en el apartado 2.2.2., al comentar las "infracciones y sanciones"). En concreto, estos procedimientos se seguirían cuando un afectado "reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica" (art. 63.1).

En el supuesto de que la autoridad de control no tramite la reclamación o no resuelva transcurridos tres meses desde que se presentó la solicitud, el interesado tendrá derecho a ejercer la tutela judicial efectiva, dirigiéndose a los tribunales del Estado en que esté

[121] RECIO GAYO, "Los derechos a presentar reclamaciones ante la autoridad de control y a la tutela judicial efectiva", en *Reglamento General de protección de datos. Hacia un nuevo modelo euroeo de privacidad, op.cit.,* pp. 539-553.

establecida la autoridad de control (art. 78 RGPD). Sin embargo, nuestra legislación[122] prevé la posibilidad de interponer (en vía administrativa) un recurso de reposición previo al recurso contencioso-administrativo. Del mismo modo, estas acciones judiciales podrán interponerse contra el responsable o encargado del tratamiento del Estado en el que éste tenga su residencia, "a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos" (art. 79 RGPD).

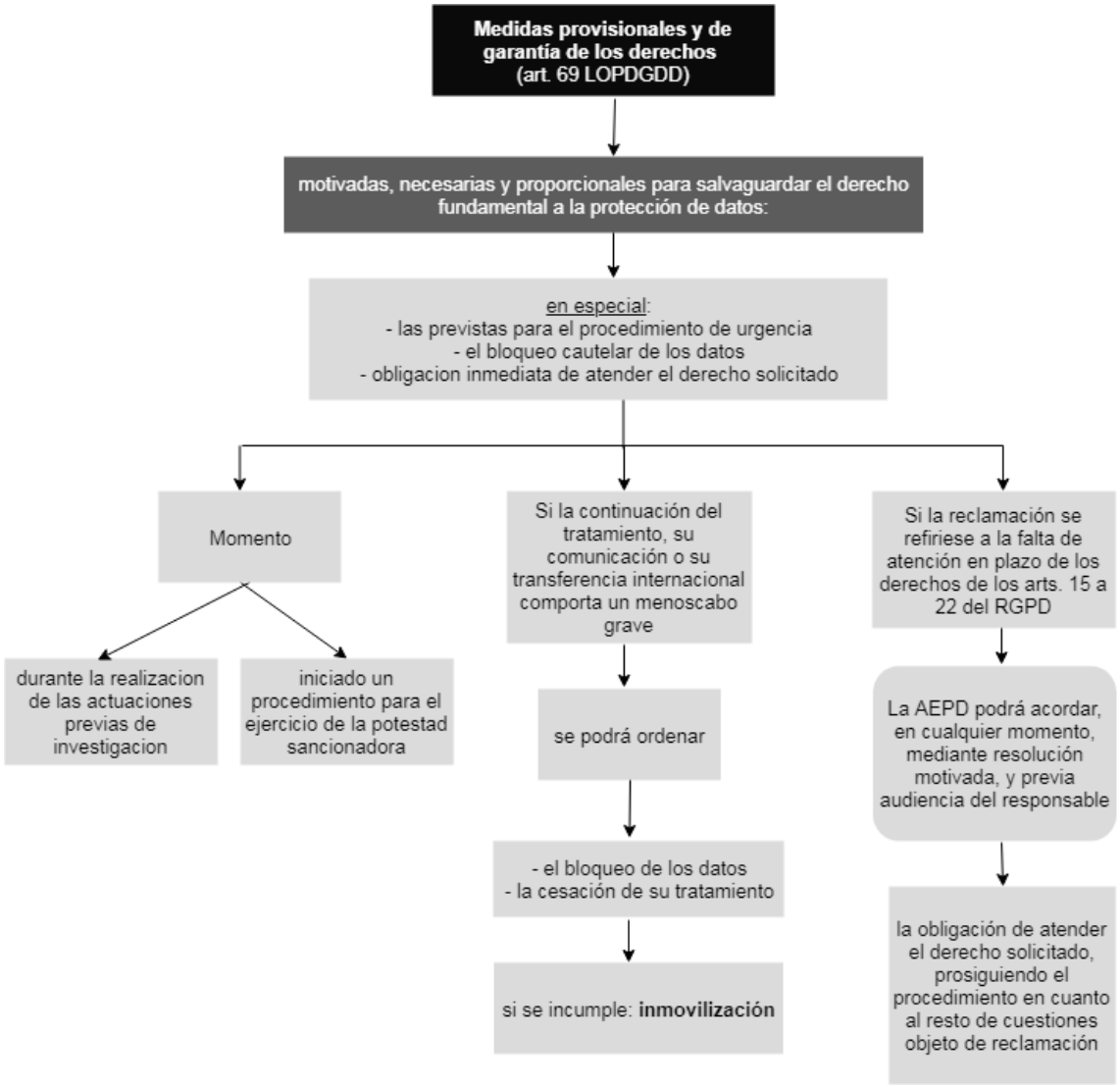
Para ambas situaciones de reclamación (ante la autoridad de control o ante el responsable o encargado del tratamiento), siempre se podrá ejercitar cualquier otro recurso administrativo, acción judicial o extrajudicial que esté disponible.

Los interesados podrán atribuir la presentación de las reclamaciones y el ejercicio de derechos en su nombre a entidades y organizaciones cuyos objetivos sean la persecución del 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 (art. 80 RGPD).

Es posible, en algunas ocasiones, que puedan producirse duplicidades de procedimientos entre diferentes Estados Miembros, facultando a cualquier tribunal distinto al que ejercitó la acción en primer lugar para suspender su procedimiento (art. 81 RGPD).

[122] Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa.

El siguiente cuadro podemos ver un diagrama comprensivo de las situaciones que pueden darse en el ámbito de las medidas[123]:



[123] Iberley.es. Accesible en: https://www.iberley.es/temas/medidas-provisionales-garantia-derechos-materia-proteccion-datos-lopdgdd-62826.

2.1.2. AUTORIDADES DE CONTROL INDEPENDIENTES

La necesaria existencia de autoridades independientes en el control de la protección de datos personales deriva de la propia CDFUE, declarando que el respeto a las normas, que incluye en el art. 8, estarán sujetas al control de una autoridad independiente (apartado 3º).

La Directiva 95/46/CE instituyó el deber general de notificar el tratamiento de datos personales a las autoridades de control, sin embargo, la institución de las mismas no implicó en todos los casos una mejora en la protección de datos. Esto obligó al legislador europeo a prever esta situación con la finalidad de encontrar procedimientos y mecanismos que satisfagan la necesidad de contar con medios eficaces que se centren en el tratamiento de aquellos datos que pudieran entrañar un riesgo para las libertades y los derechos fundamentales relacionados con la protección de datos, en particular, los tratamientos que implican las TICs[124].

El control del procesamiento de datos se encuentra bajo la órbita de las Autoridades de Protección de Datos, siendo estas públicas e independientes, que tienen bajo su órbita el poder de supervisión, investigación y corrección, para asegurar la eficaz protección de los derechos derivados del tratamiento de datos personales y la aplicación de la legislación en la materia. Estas autoridades brindan asesoramiento en todos los asuntos relacionados con la protección de datos y son las encargadas de tramitación de las reclamaciones presentadas por el incumplimiento de la legislación nacional correspondiente.

Para asegurar un grado coherente de protección de los datos personales de todos los individuos de la UE y para evitar conflictos que dificulten la libre circulación de datos entre los Estados miembros, el Parlamento Europeo, aprobó el nuevo Reglamento proporcionando seguridad jurídica y la transparencia necesaria y para garantizar el mismo nivel de protección de derechos y de obligaciones exigibles, estableciendo las mismas responsabilidades de todos los responsables y encargados del tratamiento, así como un grado equivalente de sanciones en todos los Estados de la Unión.

Por otra parte, el RDGP otorga la libertad a cada Estado miembro de establecer el número de Autoridades de Control conforme a su derecho interno, con el fin de respetar la

[124] Considerando 89 RGPD.

estructura constitucional de las competencias administrativas; siendo una sola la que represente y sea su interlocutora por cada Estado.

Estas Autoridades de control deberán ofrecer un asesoramiento experto en asuntos relacionados con la protección de datos y deberán tramitar las reclamaciones presentadas ante la vulneración de algún derecho con ocasión de la violación del RGPD y de las legislaciones internas, en nuestro caso la LOPDGDD. Así mismo, deberán asesorar o responder las preguntas que le presenten las empresas u organizaciones que traten datos. Para responder o asesorar a una empresa u organización, será competente la autoridad de control del Estado miembro en que dicha empresa u organización tenga su sede. No obstante, si esta realiza el tratamiento de datos en más de un Estado o si es parte de un grupo de empresas establecidas en más de un Estado miembro de la Unión Europea, la autoridad competente será la del Estado que se haya establecido al efecto.

En virtud del artículo 57 RGPD, la Autoridad de control será la responsable, dentro de su territorio, de controlar la aplicación del Reglamento, así como promover la difusión del mismo y de su contenido, haciendo principal hincapié en los derechos, garantías y riesgos sobre el tratamiento de datos, principalmente cuando se refieran a actividades dirigidas a los niños. Del mismo modo deberá, a solicitud de parte, facilitar la información sobre el tratamiento del que están siendo objeto sus datos y en caso de ser presentada una reclamación, deberá investigar, resolver e informar en un plazo razonable sobre las actuaciones.

Además, las Autoridades de Control deberán llevar un registro de sus actividades y deberá presentar un informe anual frente a la autoridad competente, ya sea el Parlamento nacional, el Gobierno o la autoridad designada de conformidad con el derecho interno de cada Estado. Posteriormente dicho informe deberá ponerse a disposición del público, de la Comisión y del Comité[125].

El RGPD establece que cada Estado miembro deberá establecer una o varias autoridades públicas independientes, que serán las responsables de supervisar la aplicación del Reglamento, con la finalidad de hacer efectiva la protección de los derechos vinculados al tratamiento de los datos personales y de facilitar la libre circulación de los datos dentro

[125] Art. 57 RGPD.

del bloque. El RGPD, por tanto, habilita a los Estados miembros a establecer la cantidad necesaria de autoridades de control, de modo que pueda reflejar su estructura constitucional, organizativa y administrativa[126]. Por otro lado, los poderes o facultades de estas autoridades se encuentran regulados en el artículo 58 del Reglamento, sin perjuicio de los que les puedan ser asignados en virtud de leyes internas.

Cada estado miembro de la UE deberá tener al menos una Autoridad de control, que tendrá competencia cuando los datos son tratados dentro de su jurisdicción, incluso cuando se trata de una sociedad que opera en más de un Estado miembro o es parte de un grupo de una sociedad parte de un grupo presente en más de un Estado miembro, siempre que los datos hayan sido gestionados dentro de su jurisdicción. En tal sentido, el TS, con ocasión al recurso de casación presentado por la directora de la Agencia Española de Protección de Datos (AEPD), establece que:

> "(…) *A los efectos de considerar si es aplicable la normativa de protección de datos de carácter personal de un Estado miembro de la Unión Europea a una empresa responsable del tratamiento de datos personales, en aquellos supuestos en que la sede principal esté ubicada en el territorio de otro Estado miembro de la Unión Europea, pero que realice actividades en otros Estados miembros, el concepto de tratamiento …debe interpretarse de forma flexible y antiformalista, en el sentido de que resultan comprendidos el tratamiento de datos personales que se realiza en el marco o en el contexto de la actuación desarrollada en un Estado miembro de la Unión Europea (distinto a donde tiene la sede o administración principal) a través de la utilización de medios instrumentales que se revelen idóneos y eficaces en el tratamiento de datos personales*"[127].

Cuando un Estado establezca más de una autoridad de control, deberá establecer legalmente los mecanismos para el funcionamiento de las mismas, manteniendo la coherencia exigida; designando " (…) *la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se*

[126] Art. 51 RGPD.
[127] STS de 5 de febrero de 2019.

refiere el artículo 63"[128], y esta autoridad será el único punto de contacto oficial, entre las distintas autoridades del mecanismo de control y coherencia con el Comité y la Comisión.

En el caso de España particularmente, existe más de una autoridad de control, como reflejo de nuestra estructura constitucional, organizativa y administrativa. A nivel Estatal, la autoridad de Control es la Agencia Española de Protección de Datos (AEPD), mientras, a nivel autonómico, se encuentran: la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de varias Comunidades Autónomas, que poseen personalidad jurídica propia, plena autonomía y absoluta independencia en el ejercicio de sus funciones, como veremos seguidamente.

2.1.2.1. Independencia

Como señalan PIÑAR MAÑAS Y RECIO GAYO[129], las autoridades de control de datos desde su inicial contemplación en el artículo 28 de la Directiva 95/46/CE hasta su inclusión en el art. 51 RGPD, constituyen los "auténticos guardianes de los derechos y libertades fundamentales relativos al tratamiento de datos personales". Así, "buena muestra de la importancia de las autoridades de control es que tanto el art. 8.3 de la CDFUE como el art. 16.2 TFUE -por tanto Derecho primario de la Unión- establecen que el respeto a las normas de protección de datos personales debe estar sujeto al control de una autoridad independiente"[130].

De forma que, su independencia ha sido un tema de especial trascendencia sobre la que el TJUE se ha pronunciado en distintas ocasiones; en concreto, lo ha hecho sobre el indicado artículo 28 de la Directiva 95/46/CE[131] en tres importantes sentencias:

---

[128] Art. 51.3 RGPD.

[129] PIÑAR MAÑAS, J.L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de justicia de la Unión Europea*, Wolters Kluwer, Madrid, 2018, pp. 252 y ss.

[130] TRONCOSO REIGADA, A., "Autoridades de control independientes", en *Reglamento general de protección de datos*…", *op.cit*., pp. 472 y ss.

[131] El indicado precepto establece lo siguiente:

"Artículo 28. Autoridad de control

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia".

La sentencia de 9 de marzo de 2010, caso Comisión/Alemania, asunto C-518/07, la de 16 de octubre de 2012, caso *Comisión/Austria*, asunto C-614/10, y, por último, la de 8 de abril de 2014, caso *Comisión/Hungría*, asunto C-288/12.

Las dos primeras sentencias, la de 9 de marzo y la de 16 de octubre, el Tribunal de Justicia dio una interpretación autónoma y amplia de la expresión "con total independencia", prevista en el art. 28.1, segundo párrafo de la Directiva, al señalar, que la misma debe interpretarse "en el sentido de que se opone a la tutela del Estado"[132]; por lo que "procede declarar que la República Federal de Alemania ha incumplido las obligaciones que le incumben en virtud del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46, al someter a la tutela del Estado a las autoridades de control competentes para vigilar a los diferentes *Länder* el tratamiento de datos personales en el sector no público, y al haber adaptado así incorrectamente su normativa nacional a la exigencia de que dichas autoridades ejerzan sus funciones con "total independencia"[133].

La sentencia de 8 de abril de 2014, *Comisión/Hungría,* viene a suponer una continuidad de las dos anteriores, al plantearse la cuestión relativa al alcance de la independencia de las autoridades de control, con especial incidencia en los conceptos de supervisión jerárquica y obediencia anticipada. Uno de los aspectos manejado en la sentencia es el del presupuesto de la autoridad Húngara de control de datos (DSK), señalando que "no es necesario que el DSK disponga de una línea presupuestaria autónoma (…) para poder cumplir el requisito de independencia establecido en el artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46"; no obstante, "la atribución de los medios humanos y materiales que necesita la autoridad de control no debe impedir que ejerza sus funciones "con total independencia" en el sentido del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46"[134]. Por todo ello, concluye el Tribunal que "la República de Austria ha incumplido las obligaciones que le incumben en virtud del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46, al no haber adoptado todas las medidas necesarias para que la legislación vigente en Austria cumpla el requisito de independencia por lo que se refiere a la DSK"[135]. Lo cual implica, que haya de tenerse en cuenta un concepto amplio

[132] Apartado 55.
[133] Apartado 56.
[134] Apartado 58.
[135] Apartado 66.

de independencia, por el que no sea suficiente con que se garantice la independencia funcional para cumplir con la "independencia total" requerida a las autoridades de control de protección de datos.

En esta sentencia, se pronuncia, igualmente, el Tribunal sobre la obligación de respetar el mandato de la autoridad de control hasta su expiración y de poner fin antes del tiempo al mismo únicamente cuando se observen las normas y garantías de la legislación aplicable ("cuando concurra un motivo grave y objetivamente verificable"[136], "por tratarse de un requisito primordial de su independencia".

El RGPD considera como un elemento esencial para la protección de los datos la plena independencia de las autoridades de control y el establecimiento de las mismas en todos los Estados; lo que no implica que estas, como muestra de su independencia, queden exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial (Considerando 117). Así, cada una de estas autoridades y cada miembro de dicha autoridad gozará de total independencia de cualquier injerencia externa y no podrán solicitar ni admitir instrucción alguna. Del mismo modo, los miembros de estas deberán abstenerse de realizar cualquier acto que pudiera resultar incompatible con su función o que pudiera generar un conflicto de intereses, sea este acto a título oneroso o gratuito[137].

Por su parte cada Estado miembro deberá garantizar a cada autoridad de control el acceso a los recursos humanos, económicos y financieros, así como la infraestructura necesaria para el fiel cumplimiento de sus deberes, no obstante, deberá abstenerse de interferir en sus actuaciones y en la designación del personal, de modo de garantizar la verdadera independencia. Asimismo, deberá aprobar el presupuesto de dicha autoridad dentro del presupuesto general, sin que ello implique una interferencia en su accionar.

La independencia de los órganos de control en el derecho comparado se encuentra prevista legalmente de distintas formas, tanto en cuanto a la conformación de los órganos como en referencia al nombramiento de sus miembros[138]. En países como Francia, Italia

[136] Apartado 55.
[137] RGPD, Capítulo VI.
[138] PUENTE ESCOBAR, A., "La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal", *Azpilicueta. Cuadernos de Derecho*, San Sebastián, 2008, pág. 26.

y Portugal los órganos de control colegiados se encuentran integrados por representantes de los distintos poderes; en tanto, en el caso de países como Hungría y República Checa, las mencionadas autoridades son designadas directamente por el Parlamento e incluso, en República Checa, además de designar al director, compete al parlamento designar determinados grupo de funcionarios del órgano; mientras en países como Austria o Países Bajos los órganos rectores de estas autoridades son nombrados por el propio gobierno, sin menoscabar la independencia técnica de estos.

Otra garantía que ofrece el Reglamento sobre la independencia de las autoridades es la exigencia de que los miembros de las autoridades de control deberán ser nombrados después de un proceso transparente y las condiciones que le serán aplicables deberán ser establecidas por leyes internas de cada Estado. Deberá garantizarse la independencia de sus miembros, y para ello, entre otras regulaciones, se establece la imposibilidad de ejercer cualquier actividad incompatible a su función durante su mandato. La autoridad de control deberá contar con personal propio seleccionado por esta directa o indirectamente, para lo que cada Estado deberá dotar a las autoridades de control de los recursos humanos y financieros, y de la infraestructura necesaria para el cumplimiento eficaz de sus funciones.

En España, la AEPD no se encuentra bajo relación jerárquica de ningún órgano o poder del Estado, ni se encuentra incluida en la estructura orgánica de ningún otro órgano de la Administración del Estado, tal como sucede en otros organismos controladores, como la Comisión Nacional del Mercado de Valores, la Comisión Nacional de las Telecomunicaciones, la Comisión Nacional de la Energía o el Tribunal de Defensa de la Competencia[139]. Así, su independencia se encuentra establecida en la LOPDGDD (artículo 44.1) y en el artículo 1.2 del Estatuto de la Agencia[140]: "*La Agencia de Protección de Datos actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones (…)*".

[139] PUENTE ESCOBAR, *op.cit.,*. pp. 26 y 27

[140] Aprobado por Real Decreto 428/1993, de 26 de marzo.

2.1.3. SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (SUEPD)

Para los actos comunitarios relacionados con el tratamiento y protección de datos personales y la libre circulación de estos, el TFUE establece que sean aplicables las instituciones y organismos de la Unión[141]. Del mismo modo, dispone la existencia de un organismo independiente con funciones de control y vigilancia sobre la aplicación de los actos comunitarios de las instituciones y organismos de la Unión Europea[142]. Al igual que se ha pronunciado la jurisprudencia del TSJUE, declarando el principio de "total o absoluta independencia" de las autoridades de protección de datos como uno de los pilares esenciales sobre los que descansa el sistema de garantías del derecho fundamental a la protección de datos personales[143]. En base a este principio básico se sustenta jurídicamente la creación del organismo Supervisor Europeo de Protección de Datos.

Este organismo fue concebido inicialmente como una mera autoridad de control por el Parlamento Europeo y la Comisión, hasta que el Consejo Económico y Social Europeo recomendó incluir la independencia de esta autoridad como un elemento fundamental de su existencia[144].

Así, el artículo 41 del Reglamento 45/2001/CE crea la figura del Supervisor Europeo de Protección de Datos[145], estableciendo la potestad exclusiva del Parlamento y del Consejo, actuando en forma conjunta de nombrar al SUEPD y al Supervisor adjunto.

---

[141] Antiguo artículo 286 del Tratado Constitutivo de la Unión Europea. DOCE de 24 de diciembre de 2002. C 325:
"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea". Capítulo I. Legislación y Supervisión en Europa.

[142] El Art. 16.2. TFUE establece que las normas que se establezcan por el Parlamento y el Consejo sobre el tratamiento de datos personales por las instituciones europeas y Estados miembros estarán sometidas al control de autoridades independientes.

[143] Así, en tres ocasiones se ha declarado por la Comisión la no concurrencia de "absoluta independencia". Este es el sentido sobre el que se han pronunciado las sentencias de 9 de marzo de 2010: asunto C-518/07, Comisión v. Alemania; 16 de octubre de 2012, asunto C-614/10, Comisión v. Austria, y 8 de abril de 2014, asunto C-288/12, Comisión v. Hungría.

[144] Dictamen CESE. DO.C.51 de 23 de febrero de 2000. Recomendación 3.11.1: "(…) debería precisarse que "se instituye una autoridad independiente de control (…)".

[145] Artículo 41 Reglamento 45/2000, de 18 de diciembre de 2000:

Su régimen jurídico se establece en el propio Reglamento, así como sus funciones y competencias, que se definen en los arts. 46 y 47 del mismo.

2.1.4. AUTORIDADES NACIONALES Y AUTONÓMICAS

Con bastante paralelismo entre la figura anterior del SUEPD con la de las autoridades nacionales y autonómicas (y las de éstas últimas entre sí), pasamos a continuación al examen de estas, en las que, como veremos, las autoridades autonómicas constituyen un reflejo de la autoridad nacional, en cuanto a las funciones y desarrollo de su actividad, además de, por supuesto, su independencia del resto de los poderes públicos. En este sentido, la utilización de sus instrumentos interpretativos de actuación, a través de Informes, Circulares, Resoluciones o Criterios, supone un importante medio de enriquecimiento en la interpretación de la normativa sobre protección de datos y, en concreto, de la de transparencia pública, en el acceso a la información pública, como tendremos ocasión de ver en el Título II de este trabajo.

2.1.4.1. **La agencia española de protección de datos**

La AEPD es la autoridad de control nacional en materia de protección de datos en España, creada por la LORTAD. La LOPDGG, en su Cap. I, arts. 44 a 56, contiene la regulación vigente de la AEPD, dejando inaplicable la anterior regulación contenida en la LOPD, completándose con lo dispuesto en la LRJSP[146].

"1. Se instituye una autoridad de control independiente denominada "Supervisor Europeo de Protección de Datos". 2. Por lo que respecta al tratamiento de los datos personales, el Supervisor Europeo de Protección de Datos velará porque 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. El Supervisor Europeo de Protección de Datos garantizará y supervisará la aplicación de las disposiciones del presente Reglamento y de cualquier otro acto comunitario 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 comunitario, y asesorará a las instituciones y a los organismos comunitarios, así como a los interesados, en todas las cuestiones relacionadas con el tratamiento de datos personales. Con este fin ejercerá las funciones establecidas en el artículo 46 y las competencias que le confiere el artículo 47".

[146] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Le corresponde realizar las funciones establecidas en los arts. 57 y 58 del RGPD, así como aquellas otras que le sean atribuidas por ley estatal o de la UE. Asimismo, llevará a cabo actividades de investigación, conforme a lo previsto en el título VIII de la LOPDGDD, así como planes de auditoría preventiva, referidos a un sector concreto de actividad, los cuales "(…) *tendrán por objeto el análisis del cumplimiento de las disposiciones del RGPD y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría*" (art. 54). Además, tendrá otras potestades de regulación, como la emisión de Circulares, en las que se fijen los criterios de actuación conforme al RGPD.

El Presidente de la Agencia (y el Adjunto) serán nombrados (por un mandato de cinco años, renovable) por Real Decreto a propuesta del Ministro de Justicia, entre personas de reconocida valía profesional, sobre todo en materia de protección de datos, aunque, previamente, la propuesta del Gobierno se remitirá a la Comisión de Justicia del Congreso, que "deberá ratificar en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, 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"[147]. El presidente estará asesorado por un Consejo Consultivo, compuesto por los integrantes determinados en el art. 49.

"*Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la AEPD informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación*" (art. 52.1).

[147] Art. 48.3 LOPDGDD.

2.1.4.2. Autoridades autonómicas de control

Al igual que la AEPD, las Agencias de las CCAA tienen la consideración de Autoridades de control, gozando de independencia y objetividad en el ejercicio de sus funciones; garantías establecidas por las distintas leyes autonómicas creadoras de las instituciones. A nivel autonómico, encontramos las siguientes entidades dotadas de personalidad jurídica propia y plena autonomía e independencia en el ejercicio de sus funciones:

- La Autoridad Catalana de Protección de Datos,
- La Agencia Vasca de Protección de Datos y
- El Consejo de Transparencia y Protección de Datos de Andalucía

Estas entidades, realizarán, al igual que la AEPD, las funciones y potestades previstas en los arts. 57 y 58 RGPD, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía (art. 57.1).

Así, su competencia puede extenderse incluso, al control de los tratamientos de datos a cargo de entidades del sector público, dependiendo del organismo que ostente esa autoridad y que esa institución esté incluida dentro del ámbito de una autoridad autonómica de control previamente constituida.

La ubicación de los ficheros es determinante para la atribución de competencias, ya que no se asignan a ciertas entidades por su función, sino que el control lo ejerce la comunidad autónoma o entidades locales, cuyos ficheros hayan sido creados o gestionados en su ámbito territorial.

Aunque el tratamiento lo realice el responsable del fichero o un tercero por cuenta de aquél, la competencia viene dada por el titular del fichero, en la medida en que esa entidad se encuentre dentro del ámbito de actuación de la autoridad autonómica correspondiente. De forma que si el tratamiento realizado por el encargado no se hace sobre la base de datos a su cargo sino sobre la de otros, como los ficheros comunes, por ejemplo, la competencia de control es de la AEPD directamente, a quien las autoridades autonómicas están obligadas a comunicar los contratos de prestación de servicios de tratamiento antes de su perfeccionamiento; obligación que no está prevista para otras entidades ni otros encargados de tratamiento (artículo 43)[148].

Las funciones de las autoridades autonómicas de protección de datos se extienden, en el marco de su competencia, hasta considerarlos sujetos de la acción exterior (artículo 56), como la AEPD, para celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, en consonancia a lo establecido en la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

2.2 SISTEMA SANCIONADOR

2.2.1. INFRACCIONES Y SANCIONES

En cuanto a las infracciones, reguladas tanto en el RGPD, como en la LOPDGDD, se recogen en los artículos 83 y 84, y 71 a 74, respectivamente.

[148] FARRÉ TOUS, S., "Principios de la protección de datos: acceso a los datos por cuenta de terceros. El encargado del tratamiento en el ámbito de las administraciones públicas", en *Comentario a la ley de protección de datos*, comentario al art. 12 LOPD, *op.cit.*, pp. 1103-1125.

Así, el RGPD introduce de forma detallada un nuevo régimen que viene a suponer novedades importantes en relación con la Directiva 95/46 y la LOPD; no obstante, dejar importantes dudas en diversas cuestiones como veremos seguidamente[149].

Como señala CORRAL SASTRE[150], de acuerdo con el art.11 del Reglamento, uno de los objetivos principales del nuevo régimen sancionador (considerando el art. 11 del RGPD) es que, partiendo de que la vulneración de este derecho fundamental se sancione en todos los Estados miembros, se consiga una armonización en la aplicación de las sanciones, de forma que sean equivalentes (económicas o no) entre todos los Estados de la Unión, impidiendo la existencia de regulaciones dispares, evitándose la impunidad sancionadora mediante los llamados "paraísos de datos"[151] dentro de la UE, que puedan limitar la circulación de datos, impidiendo el ejercicio de la actividad económica, falseando la competencia, de forma que se impida ejercer a las autoridades las funciones que les atribuye el Derecho de la Unión (Considerando 9).

Con la finalidad de que se lleve a cabo una mejor aplicación de las disposiciones contenidas en el RGPD por parte de las Autoridades de control, el GT29 ha publicado unas Directrices, las cuales habrá que conciliar con la propia normativa nacional, en nuestro caso con la LOPDGDD[152].

Así, estas directrices comienzan por resaltar lo esencial que resulta para disponer de un régimen armonizado de protección de datos el que se lleve a cabo una ejecución coherente y adecuada de las normas sobre protección de datos; de forma que la imposición de multas administrativas, junto con las medidas previstas en el art. 58, como instrumento a disposición de las autoridades de control, suponen un elemento esencial del nuevo régimen sobre protección de datos. Como principios básicos contemplados en estas directrices, destacamos los siguientes:

[149] Para más información sobre el Régimen sancionador en materia de protección de datos, vide la obra de los profesores PIÑAR MAÑAS J.L., y CANALES GIL, A., *Legislación de protección de datos*, Iustel, 2º ed., 2011.

[150] CORRAL SASTRE, A., "El régimen sancionador en materia de protección de datos en el Reglamento General de la UE", en *Reglamento General de Protección de Datos*…, pp. 573 y ss.

[151] Al igual que su equivalente económico-fiscal en los "paraísos fiscales", los paraísos de datos suponen ciertos reductos en los que la normativa sobre protección de datos se hace menos exigente con la finalidad de acoger más empresas en el país de que se trata.

[152] GT29, "Directrices sobre la aplicación y fijación de multas administrativas a efectos del Reglamento 2016/679", adoptadas el 3 de octubre de 2017.

- 1º. La infracción del Reglamento debe dar lugar a la imposición de sanciones equivalentes en todos los Estados miembros.
- 2º. Las multas administrativas deben ser efectivas, proporcionadas y disuasorias.
- 3º. La evaluación por la autoridad de control se realizará para cada caso concreto.
- 4º. A fin de llevar a cabo una ejecución armonizada de las sanciones es necesario la participación activa y el intercambio de información entre autoridades de control.

A nivel general el RGPD, en su artículo 83, establece las condiciones para la imposición de multas administrativas, las cuales deberán ser examinadas en función de cada caso concreto, lo que pone de manifiesto una decidida apuesta por la responsabilidad proactiva o *accountability (*Considerando 85 y art. 5.2. del Reglamento*)*, como criterio inspirador del régimen sancionador, ya implantado en España por la modificación de la LOPD, en 2011[153]. Las multas deberán ser efectivas, proporcionadas a la infracción que sancione y deberán, a su vez, tener un carácter disuasorio, pues el fin no es sancionar sino prevenir las situaciones en las que se vulneren los derechos protegidos en el Reglamento.

Para establecer la cuantía, y que ésta verdaderamente sea proporcionada y disuasoria, se deberá atender a la naturaleza, gravedad y duración de la infracción, para lo que se tendrá especial consideración: la influencia sobre el ámbito de afectación en el tratamiento de datos de que se trate, así como la categoría de datos tratados, la cantidad de individuos perjudicados y el grado de daños y perjuicios que hayan sufrido.

El RGPD tipifica como infracciones los actos y conductas establecidos en los apartados 4, 5 y 6 del artículo 83 y la LOPDGDD en el Título IX. Para el RGPD es relevante establecer la cuantía o el grado de infracción base al grado de conciencia, intencionalidad o negligencia del infractor y la reincidencia de trasgresiones al instrumento. Además, deberá tenerse en cuenta otras circunstancias, como la evaluación del grado de responsabilidad del responsable y del encargado del tratamiento de datos en el cumplimiento de sus funciones relacionadas a las medidas técnicas y organizativas que hubieran aplicado, así como cualquier factor agravante de la infracción. Al mismo tiempo, se tendrá en consideración si éstos hubieran tomado medidas para atenuar los daños y

[153] PIÑAR MAÑAS, J.L., "La importante reforma del régimen sancionador en materia de protección de datos: reflexiones urgentes", *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 50, 2011.

perjuicios, el grado de cooperación con la autoridad de Protección de Datos con la finalidad de enmendar la infracción y mitigar los daños provocados y cualquier otro factor atenuante de la responsabilidad o efectos de la infracción.

En cuanto al establecimiento de cuantías, el Reglamento únicamente alude al incumplimiento de las condiciones para el consentimiento para establecer la sanción, destacando el sustancial aumento de la cuantía de las multas administrativas hasta llegar a la llamativa cifra para personas y empresas de 20.000.000 € o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, si estamos ante una empresa; opción que, como señala CORRAL SASTRE parece estar dirigida a multinacionales del sector de las tecnologías de la información, que, de otra forma, sería casi imposible disuadir económicamente. Planteándose, en atención al principio de proporcionalidad, si, al igual que sucedió con la LOPD[154], que se llegó a tachar de inconstitucional el sistema sancionador por atentar contra este principio[155], si sucede lo mismo con el régimen de multas impuesto por el RGPD, a lo que debe responderse que no parece que se infrinja este principio, en la medida en que los criterios de imposición de sanciones resultan de las sentencias del TJUE; siendo, en algunos sectores, de mayor cuantía, como las que se producen en el ámbito de la competencia[156].

Siguiendo con el análisis del Reglamento, la traslación del principio de tipicidad en relación con las infracciones llega a generar importantes dudas; en la medida en que no existe tipificación directa[157], ya que no se recogen en preceptos concretos las conductas a sancionar, sino que hay una remisión a otros preceptos de esta misma norma, en los que se señalan las obligaciones a cumplir por los sujetos afectados; cuyo incumplimiento determina la comisión de la infracción. Del mismo modo, la aplicación de este principio a la imposición de sanciones genera mayores dudas, en la medida que éstas delimitan por

[154] Que debe entenderse que no queda desplazada completamente, por cuanto se seguirá aplicando "en aquellos ámbitos que queden fuera del ámbito de aplicación de la norma europea y, en los casos en que el Reglamento deje margen normativo a los Estados.

[155] TORNOS MÁS, J., "Potestad sancionadora de la Agencia Española de Protección de Datos y principio de proporcionalidad", en *Potestad sancionadora de la Agencia Española de Protección de Datos*, Thomson Aranzadi, 2008, p.33.

[156] CORRAL SASTRE, A., *op.cit*., p. 576.

[157] Consiste en la técnica de "tipificación remisiva expresa", aceptada generalmente. Para más información ver el trabajo del profesor NIETO GARCÍA, A., "Derecho Administrativo sancionador", Tecnos, 2012, p. 313.

el Reglamento de forma excesivamente amplia; que, como señala CORRAL SASTRE[158], supone "una inseguridad jurídica inaceptable e incompatible con el principio de tipicidad de las sanciones, tal y como lo interpreta el TC, amén del excesivo margen que se otorga a las autoridades de control a la hora de imponer las correspondientes multas".

Por último, destaca, en nuestro análisis del Reglamento, la ausencia de un régimen de prescripción de infracciones y sanciones que hubiera dotado de mayor certeza al sistema; lo que, igualmente, puede tener una influencia decisiva en la seguridad jurídica. Como veremos al tratar la LOPDGDD, serán sus prescripciones las que nos determinen este régimen.

Una vez conocido el sistema de infracciones establecido en el RGPD es necesario estudiar el sistema establecido por la LOPDPGDD, para lo que haremos una breve reseña sobre los tres tipos de infracciones que prevé.

En primer lugar, se encuentran las infracciones muy graves, para cuando se trate de un incumplimiento sustancial. En este grupo se encuentran las violaciones reguladas en el artículo 83.5 y 83.6 del RGPD y se incluyen, entre otras, el tratamiento de datos personales vulnerando los principios y garantías establecidos en el Reglamento, así como cuando esto ocurre sin base legal que lo sustente, o cuando el consentimiento no cumpla con los requisitos de validez. Así mismo, se incluyen en este grupo, el tratamiento de datos con una finalidad distinta a la que fueron obtenidos, incompatible con ésta y sin el consentimiento del titular o cualquiera de las demás bases legales que lo legitimen.

Además, se considera infracción muy grave el tratamiento de datos de salud (y, por tanto, de los datos especial protección) cuando no se encuentren presentes las circunstancias establecidas en el artículo 9 de la ley nacional, así como el tratamiento de datos personales relacionados a medidas de seguridad conexas o tipos penales como condenas e infracciones que no se encuentren en el artículo 10 LOPDGDD.

En segundo lugar, regula las infracciones graves, previstas para los casos de vulneración sustancial. Aquí ya no se trata de supuestos de incumplimiento de la norma, sino de vulneraciones de los derechos de los individuos, por falta de previsiones o adopción de las medidas necesarias para garantizarlos. En este grupo encontramos las infracciones

[158] CORRAL SASTRE, *op.cit.*, p. 579.

establecidas en el artículo 83.4 del RGPD y las especificadas en la LOPDGDD. A modo de ejemplo de estas últimas se señalan: las infracciones que devengan de la falta de adopción de las medidas necesarias para verificar la validez del consentimiento, el tratamiento de los datos de los menores de edad sin el consentimiento de su responsable legal o el propio cuando hubiera cumplido la mayoría, la falta de previsión y de adopción de la medidas técnicas y organizativas necesarias para realizar el adecuado tratamiento de datos.

Del mismo modo son consideradas infracciones graves la obstaculización: el impedimento, o la no atención reiterada de los derechos fundamentales de acceso, rectificación, supresión, limitación del tratamiento; así como la contratación de un encargado que no ofrezca las garantías suficientes de idoneidad o sin autorización previa del responsable; la inobservancia o trasgresión a las medidas de índole técnico u organizativo que debieron implantarse en cumplimiento del artículo 32.1 de RGPD.

También es sancionable bajo este supuesto, si el responsable del tratamiento contrata a un encargado que no garantice suficientemente la aplicación de las medidas antes mencionadas, o encarga el trato de la información a una tercera persona sin la utilización de un contrato, en cumplimiento de lo señalado en el número 3 del artículo 28 del RGPD. De acuerdo al artículo 33 del RGPD supone una sanción en caso de no notificar a la AEPD del acontecimiento de una violación a la seguridad de los datos protegidos y la omisión de la realización de una Evaluación de impacto de las operaciones que conlleven tratamiento de datos de índole personal cuando la normativa así lo exija.

Sobre el incumplimiento de las garantías de seguridad, el TS se pronunció sobre la importancia de dichas garantías.

> *"(…) En definitiva todo responsable de un fichero (o encargada del tratamiento) debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, datos bancarios o cualquier otro dato de carácter personal pueda llegar a manos de terceras personas"*[159].

[159] SAN de 8 de abril de 2010. La sentencia desestima el recurso contencioso-administrativo interpuesto por la Asociación Española de Ingenieros de Telecomunicación contra una Resolución del Director de la AEPD de 8 de septiembre de 2009, sobre infracción en materia de protección de datos.

De lo anterior se evidencia la rigurosidad con la que las autoridades persiguen y castigan las infracciones contra la protección de datos de carácter personal, en especial las que afectan a los datos de especial protección, y las inherentes a las garantías de medidas que aseguren la integridad del manejo de los mismos.

En tercer lugar, considera infracciones leves aquellas en las que existe una transgresión meramente formal, en la que existe una omisión o incumplimiento de las formas establecidas para hacer efectiva y eficiente la protección de los datos. En este grupo encontramos las infracciones previstas en los artículos 83.4 y 83.5. Asimismo, de acuerdo a la LOPDGDD, se incluyen entre otros: no facilitar toda la información exigida por el titular, afectando a su derecho a la información, solicitar un pago para entregar la información o atender solicitudes, superior a los costes de dichas diligencias, incumplir la obligación de notificar sobre la rectificación, supresión o limitación del tratamiento de los datos personales.

Existe, a su vez, una diferencia notable entre la norma española y el RGPD, el cual prevé el derecho de indemnización que posee quién se viera afectado por daños y perjuicios de forma material o no a raíz del quebrantamiento de la legislación sobre protección de datos, como consecuencia de una infracción de la normativa por parte del responsable o encargado. Para ello las demandas de estas reclamaciones serán presentadas ante los tribunales competentes o, si se relacionara con la administración pública, será exigible de acuerdo a las normativas sobre la responsabilidad de índole patrimonial[160].

La LOPDGDD, establece, como ya se ha analizado, tres categorías de infracciones en función de su gravedad; de forma que las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2. Por ejemplo, si la contravención fue intencional o negligente, se tomará en cuenta la duración, tipología y gravedad de la contravención, así como el tipo y finalidad de operación que realice el tratamiento con la cantidad de personas afectadas, además del grado de los daños y perjuicios causados.

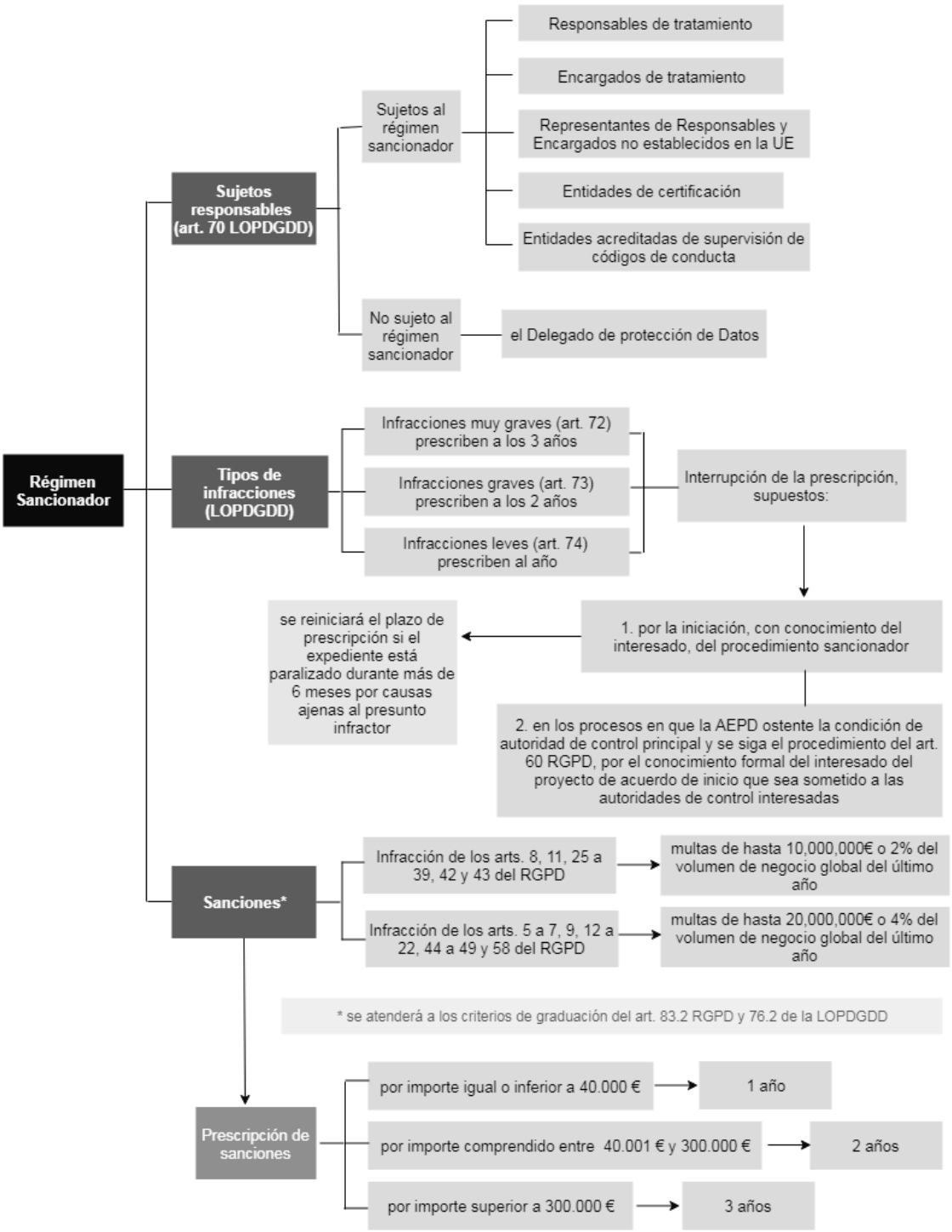
[160] Art. 65 RGPD. *"*Derecho a indemnización. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir de la institución u organismo de la Unión responsable una indemnización por los daños y perjuicios sufridos, con arreglo a las condiciones previstas en los Tratados".

Ahora bien, el término perentorio o de prescripción de las sanciones, de acuerdo a la LOPDGDD será de un año, en el caso de aquellas con valor igual o menor a 40.000; dos años para aquellas con cuantías entre 40.001 y 300.000 euros, y tres años para las sanciones cuyo valor total supere los 300.000 euros. El plazo para que las sanciones prescriban será contado a partir del día siguiente a la ejecución de la resolución que la impone o cuando el plazo para la interposición de recursos se haya cumplido. El plazo para prescribir será interrumpido cuando se inicie, previo conocimiento del interesado, el procedimiento ejecutorio, retomando su actividad si este estuviere paralizado por un tiempo mayor a seis meses debido a causas ajenas al contraventor. En relación con las infracciones de carácter continuado y permanente, el TS ha venido a aclarar su contenido, señalando[161]:

> *"En materia de protección de datos como la que nos ocupa, esta Sala ha distinguido, en sentencias de 7 de marzo de 2006 (recurso 1728/2002) y 20 de noviembre de 2007 (recurso 170/2003), entre infracciones continuadas, en los términos que las define el artículo 4.6 del RPEPS antes citado, y las infracciones permanentes, entendiendo como tales "aquellas conductas antijurídicas que persisten en el tiempo y no se agotan con un sólo acto, determinando el mantenimiento de la situación antijurídica a voluntad del autor" , y la sentencia de 23 de mayo de 2011 (recurso 912/2011), también contempla un supuesto que califica como infracción permanente, derivada en ese caso de mantener los datos inexactos en el fichero de morosos tras la cancelación de la deuda, con la consecuencia de considerar que el plazo prescriptivo no empieza a computarse mientras se mantiene la infracción".*

[161] STS de 24 de octubre de 2013.

En el siguiente diagrama[162] se resume gráficamente la estructura del sistema sancionador derivado de la normativa española aplicable (RGPD y LOPDGDD):



[162] IberLey Información Legal. Disponible en: https://www.iberley.es/temas/regimen-sancionador-materia-proteccion-datos-62809

Por tanto, hemos visto como el RGPD ha introducido novedades de calado en el sistema sancionador; desde la indicada elevada cuantía de las sanciones hasta un incremento de los sujetos que pueden ser sancionados. Este sistema, además, ha de ser completado por la LOPDGDD, que viene a establecer una regulación más precisa y detallada; estableciendo: los hechos constitutivos de infracciones y las sanciones, así como los plazos de prescripción de ambas (cuestiones ignoradas por el RGPD), así como los sujetos responsables (en el Título IX); entre ellos, los responsables, encargados de los tratamientos, los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea, las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta.

El hecho de que nuestro régimen sancionador haya sido calificado como de cierta dureza, debería suponer que el proceso de adaptación al nuevo régimen sea menos complicado que en otros países europeos[163].

Resaltar que no se considera sancionable al delegado de protección de datos (DPD).

2.2.2. PROCEDIMIENTO SANCIONADOR

Actualmente el considerando 148 del RGPD establece en su contenido la base normativa para el régimen sancionador, y que la LOPDGDD, en su artículo 83, complementa mediante el establecimiento de las condiciones aplicables al momento de imponer multas de carácter administrativo, atendiendo a los criterios de fijación y límite máximo, que la autoridad de control con competencia deberá fijar individualmente teniendo en cuenta todas las circunstancias concurrentes; en particular: la naturaleza, gravedad, duración de la infracción, consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones, atendiendo además a la intencionalidad o negligencia en la infracción.

El RGPD trajo consigo un sistema que configura el trámite de los procedimientos relacionados con el tratamiento de datos personales mediante el establecimiento de una ventanilla única, donde se encuentren tanto las autoridades principales de control como las otras interesadas; por lo que, además, pretende instaurar un proceso cooperador entre

[163] CORRAL SASTRE, *op.cit*., p. 584.

las autoridad de los Estados miembros de la UE, por lo que, en caso de diferencias, será el Comité Europeo de Protección de Datos quien emitirá decisiones con carácter vinculante.

Por ello, antes del trámite de cualquier procedimiento de carácter sancionatorio, es necesario determinar si el tratamiento objeto del proceso reviste un carácter transfronterizo o no, y en caso de que se determine la superación de dos o más fronteras, decidir qué autoridad protectora de datos será considerada como principal.

El RGPD se limita exclusivamente definir el régimen jurídico aplicable, señalando, además, que la agencia nacional encargada de la protección de datos tiene la posibilidad de remitir la reclamación al delegado de protección o a los organismos que, de acuerdo a lo indicado en un código de conducta[164], se encuentren encargados de la resolución de conflictos de manera extrajudicial. Prevé, además: las actuaciones que pueden realizarse con anterioridad a la investigación; el plazo con que se cuenta para tramitar los respectivos procedimientos o su suspensión si aplicare; y las medidas de carácter provisional que pueden tomarse para garantizar la tutela efectiva como, por ejemplo, el bloqueo de datos.

Por su parte, el Título VIII de la LOPDGDD (arts. 63 a 69) establece el procedimiento a aplicar en caso de la imposición de sanciones por parte de la AEPD ante una vulneración de la legislación en materia de protección de datos. Así, la ley contempla como el procedimiento podrá incoarse: bien, derivado de la comunicación a la AEPD por parte de la autoridad de control de otro Estado miembro de la UE de la reclamación formulada ante la misma[165]; o mediante distintos tipos de reclamaciones, las cuales irán precedidas necesariamente de una fase de admisibilidad mediante acuerdo de admisión o no a trámite; inadmitiendo aquellas que "(...) *no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción*" (art. 65).

[164] Para más información sobre los códigos de conducta, vide DÍAZ-ROMERAL GÓMEZ, A., "Los códigos de conducta en el Reglamento General de Protección de Datos", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* PIÑAR MAÑAS, J.L. (Director), Reus Ediciones, Madrid, 2016, pp. 389-412.

[165] En cuyo caso deberá actuar de conformidad a lo dispuesto en los artículos 56 y 60 del RGPD.

En esta fase de decisión de admisión o no de la reclamación, si la Agencia considera que no ostenta la condición de autoridad de control, deberá de forma inmediata y sin necesidad de realizar actuación alguna, remitir la reclamación a aquella autoridad de control principal que a su juicio sea competente para que realice el procedimiento oportunamente; notificando esta cuestión al interesado que formuló la reclamación.

Cuando fuesen de aplicación las normas establecidas en el artículo 60 del Reglamento el procedimiento se iniciará mediante la adopción del proyecto de acuerdo de inicio de procedimiento sancionador, del que se dará conocimiento formal al interesado, con ello se interrumpirá el plazo para prescripción, y se reiniciará si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor[166].

Después de la admisión del trámite de reclamación y en los casos en los que la AEPD actúe por iniciativa propia, antes del acuerdo de inicio, podrá ejecutarse la fase de actuaciones previas de investigación con el fin de indagar sobre los hechos y lograr una mejor determinación de estos; actuando cuando la investigación sea necesaria debido a tratamiento por un tráfico masivo de datos protegidos.

En el ejercicio de estas actividades de investigación, los funcionarios de la AEPD pueden: recabar la información precisa para el cumplimiento de sus funciones; realizar inspecciones; solicitar la exhibición o el envío de documentos o datos necesarios y examinarlos; inspeccionar los equipos, y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

Al concluirse las actuaciones, la Presidencia de la AEPD, dictará el acuerdo que inicia el procedimiento de ejercicio de la potestad de sanción, donde identificará al posible infractor si fuera persona o entidad, también se expondrán los hechos y señalará la infracción que hubiera podido cometerse y la sanción que procedería aplicar.

La Agencia podrá acordar medidas provisionales de forma motivada durante la fase de actuaciones previas de investigación o después de iniciado el procedimiento. Dichas medidas deben ser proporcionales y tendentes a salvaguardar el derecho a la protección de datos; pudiendo consistir en ordenar a los responsables o encargados del tratamiento

[166] Artículo 75 LOPDGDD.

el bloqueo de datos, o el cese de su tratamiento cuando la comunicación internacional afecta gravemente a datos personales del interesado; y, si no se cumpliera con lo ordenado, podrá proceder a inmovilizar dicha transferencia.

Cuando se hubiese presentado ante la AEPD una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento, podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación. Procederá la suspensión de los plazos previsto de tramitación cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la UE o de una o varias autoridades de control de los Estados miembros, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la AEPD.

El procedimiento de reclamación tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

CAPÍTULO II

DATOS PERSONALES EN EL ÁMBITO DE LA SALUD

1. CATEGORÍAS ESPECIALES DE DATOS PERSONALES

1.1. DATOS SENSIBLES ESPECIALMENTE PROTEGIDOS

Como hemos visto, el Convenio 108 se refiere a los datos especialmente sensibles, que deben recibir una especial protección. La regla general para ellos es la prohibición de tratamiento. Se consideran datos sensibles, entre otros[167], aquellos que revelan el origen racial, las opiniones políticas, convicciones religiosas o de otro tipo, datos de salud o vida sexual y los relativos a condenas penales.

La anterior LOPD, contemplaba en el art. 7 los llamados "datos especialmente protegidos", que han pasado a denominarse como "categorías especiales de datos", tanto en el RGPD, como en la LOPDGDD; ambos recogidos en el art. 9.

Podemos decir que la nueva regulación, en comparación con su antecesora contiene diferencias apreciables:

Así, frente a un escueto art. 7, que se refería a que "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias" (apartado.1), y a la prohibición de tratamiento de datos relativos al "origen racial, salud y vida sexual"(apartado.4), el RGPD, al que remite la LOPDGDD, proyecta un contenido más ampliado de este tipo de datos, para considerar, además, los datos que revelen: el origen étnico o racial, la afiliación sindical, la orientación sexual de las personas; e incluye novedosamente los datos genéticos, que se consideran datos de salud, y los datos biométricos dirigidos a identificar de manera unívoca a una person

[167] No se trata de una lista cerrada, sino que cada Estado podrá ampliar esta lista, así como reducirla, aunque mediante ley en base a una finalidad legítima (arts. 9 y 11 Convenio).

El RGPD se refiere a la especial protección que merecen este tipo de datos, en el considerando 51:

"(…) 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".

La especial naturaleza de estos datos se corresponde con un principio general de prohibición del tratamiento de los mismos. Sin embargo, de forma explícita deben establecerse excepciones a esta regla general:

1."(…), entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales" (Considerando 51*).*

*2."(…) cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud (*Considerando 52). *Además de la existencia de razones de interés público en el ámbito de salud pública (…)" (*Considerando 54*).*

A tenor del artículo 9 RGPD que regula el tratamiento de categorías especiales de datos, son considerados como datos sensibles los datos personales "(…) *que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física (…)*".

Así, la prohibición de tratamiento de estos datos se realiza por defecto, y dichos datos cuentan con un tratamiento especial; bien, debido a su propia naturaleza o por la relación que mantienen con otros derechos fundamentales, estableciendo disposiciones específicas

para aquellos casos en que el tratamiento pueda tener elevados riesgos para la protección de datos; bien, prohibiendo el mismo sin el consentimiento explícito del interesado. Incluso, cuentan con tan elevada protección, que el consentimiento para el tratamiento por parte del interesado puede no ser suficiente para habilitar el tratamiento cuando el Derecho de la Unión o de los Estados miembros establezcan prohibiciones específicas. En este sentido, la LOPDGDD, señala 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*[168]".

Así mismo, son excepciones justificativas al tratamiento de esta categoría de datos: cuando el tratamiento es necesario para la protección de intereses vitales del interesado, estando esté incapacitado para consentir; el tratamiento legítimo realizado por una organización sin ánimo de lucro, con finalidad política, filosófica, religiosa o sindical en relación con sus fines; o bien, que el propio interesado haya hecho públicos sus datos personales.

Del mismo modo, se contemplan en el RGPD excepciones a dicha prohibición amparadas en que el tratamiento de los datos se fundamente en la legislación vigente: para fines de diagnóstico médico y asistencia sanitaria o social, medicina preventiva o laboral; procesos judiciales; la que resulta necesaria para el cumplimiento de la legislación laboral o de seguridad social; razones de salud pública de interés público; y fines de archivos de interés público en investigaciones científicas, históricas o estadísticas (art. 9.2.h).

Por su parte, la LOPDGDD, en su preámbulo, alude a la necesaria reserva de ley para la habilitación de los supuestos previstos en el Reglamento, dejando a salvo, "(…) *las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El RGPD no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del*

[168] Art. 9 LOPDGDD.

afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica (…)".

Además, el preámbulo V de la LOPDGDD establece que mantendrá la prohibición de consentir el tratamiento de datos especialmente protegidos con el fin de almacenarlos, aun cuando reconoce que esta prohibición no impide que estos puedan ser tratados en el resto de los supuestos previstos en el RGPD. Así, determina que, por ejemplo, que "(…) *la prestación del consentimiento no dará cobertura a la creación de "listas negras" de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea".*

1.2. DATOS RELATIVOS A LA SALUD

1.2.1. ELEMENTOS CONSTITUTIVOS

La salud constituye el bien más preciado de que dispone la persona, de ahí que su garantía sea una cuestión fundamental, para lo cual el Derecho tiene que actuar propiciando que pueda preservarse esa protección a las personas; propiciando las mejores condiciones de salud y de asistencia sanitaria a las mismas y respetando la privacidad y el marco jurídico vigente.

Como veremos, la efectiva protección de la salud va a estar ligada estrechamente con la protección de datos personales, en la medida en que una utilización no correcta de sus principios y reglas normativas puede llegar a erosionar uno de los múltiples componentes sobre los que se asienta el concepto de salud. Así, una primera definición de la salud, no normativa, la encontraríamos en la Organización Mundial de Salud: "un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades".

Más concretamente, el apartado 45 de la Memoria Explicativa del Convenio 108 define "los datos de carácter personal relativos a la salud", aludiendo a su contenido, que incluye "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de

un individuo"; y pueden incluirse informaciones de un individuo de buena salud, enfermo o fallecido, además de informaciones relativas al abuso de alcohol o consumo de drogas[169]. Esta definición, alumbró la acuñada por el ya inaplicado RLOPD[170], que definía "los datos personales relacionados con la salud" como "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo (art. 5).

Por su parte, el concepto de "datos médicos", "hace referencia a todos los datos de carácter personal relativos a la salud de una persona, afectando igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas[171]".

La derogada Directiva 95/46 CE, se refería (art. 8) a los "datos relativos a la salud", que de acuerdo con el Tribunal de Justicia de la Unión Europea (TJCE)[172] debe entenderse en un sentido amplio, de forma que comprende la información relativa a todos los aspectos de salud de una persona, tanto físicos como psíquicos.

Actualmente, el RGPD define "datos relativos a la salud": como categoría especial de datos personales, merecedores de una especial protección, señalando que serían " (…) *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*" (art. 4.15).

De esta forma, en un contenido amplio[173], el concepto incluye, además de los datos que tienen relación con la salud de una persona, aquellos datos que proporcionan información

[169] Esta Memoria ha sido fuente recurrente en numerosos informes y resoluciones de la AEPD, P. ejemplo, el Procedimiento de Tutela de derechos TD/00884/2013.
Según informe 0445/2009 de la AEPD, la realización de test psicotécnicos implica un tratamiento de datos de salud. Del mismo modo, han de considerarse datos relacionados con la salud, los datos relativos a la minusvalía del afectado, la concurrencia de incapacidad laboral, su aptitud para el desempeño de un determinado puesto de trabajo o la causa que justifica una determinada baja laboral, según ha manifestado la AEPD en sus distintos pronunciamientos.

[170] Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

[171] Recomendación R (97) 5, del Comité de Ministros del Consejo de Europa.

[172] STJCE de 6 de noviembre de 2003, caso Sra. *Lindqvist*, asunto C-101/0. En este caso, el Tribunal fue consultado sobre si la indicación de que una persona se hubiera lesionado un pie y estuviera en situación de baja parcial constituía un dato personal relativo a la salud en el sentido del artículo 8, apartado 1, de la Directiva, pronunciándose el Tribunal de forma afirmativa.

[173] Coincidente con lo estimado por el GT29, Artículo "*Health data in apps and devices"*, de 9 de febrero de 2015, p. 2.

sobre lo que constituye "el estado de salud"; al que se alude por el considerando 35 del RGPD:

"(…) 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".

El propio GT29 contempla el dato de salud en cuanto se incluye alguna de las siguientes características: tratarse de datos con un contenido netamente médico; datos potenciales de sensores que, usados bien por sí mismos o unidos a otros, determinan una conclusión del estado de salud o riesgo de salud de una persona; se trate de conclusiones sobre el estado de salud de una persona (al margen de que sean certeras o no)[174].

Respecto de lo que debe entenderse por "salud pública", el propio Considerando 54 nos indica que debe interpretarse en el sentido de incluir "(…) *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 (…)*".

[174] GT29, *Health data in apps and devices*. 2015, p. 2.

Junto al concepto de datos de salud nos encontramos con una variante de los mismos: los datos genéticos. Así, siguiendo a SÁNCHEZ-CARO y ABELLÁN, puede distinguirse entre datos médicos y datos genéticos. Los primeros serían los que hacen referencia a todos los datos de carácter personal relativos a la salud de una persona y su estado de salud; mientras los genéticos, tendrían por objeto los caracteres hereditarios de la persona, o de un conjunto de personas con relación de parentesco; además de los datos relacionados con la transmisión de información genética, manifestado en un aspecto de salud o enfermedad, tengan o no carácter identificable[175].

Por su parte, el art. 4.1.3. RGPD configura los datos genéticos como una subcategoría de los datos de salud. Así, se trataría de "(…) *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*".

Sin embargo, no todos los datos genéticos hacen referencia a la salud, por cuanto algunos proporcionan información relativa a características físicas, como el color de la piel o del cabello, al sexo o a información vinculada al origen étnico[176].

En relación con la implantación de dispositivos tecnológicos en el organismo de una persona, ello, viene a suponer una fuente de generación de datos a los que habría que aplicar la normativa sobre protección de datos personales[177]. Al igual que las muestras de ADN tomadas en el lugar de un crimen pueden constituir una fuente de datos personales[178]. Todo ello, nos hace reflexionar sobre un concepto básico, la dignidad, como principio ligado de forma permanente a la historia de la humanidad y positivizado en los distintos instrumentos constitucionales de los países (art. 10.1 CE). Para Stefano RODOTÁ, existe una revolución de la dignidad, en la medida en que se diseña un nuevo estatuto de la persona acompañado de un nuevo marco jurídico de deberes

[175] SÁNCHEZ-CARO, J. y ABELLÁN, F, *Datos de salud y datos genéticos*, Derecho Sanitario Asesores, Granada, 2004. En su página 18 se hacen eco de la definición aportada por COLLADO GARCÍA-LAJARA, E., *Protección de datos de carácter personal (legislación, comentarios, concordancias y jurisprudencia)*, Comares, Granada 2000, pág. 25.

[176] SÁNCHEZ URRUTIA, A.V., "Información genética, intimidad y discriminación", *Acta Bioética*, vol.8, nº 2, 2002.

[177] Según el Grupo europeo de ética de las ciencias y de las nuevas tecnologías, en su Dictamen sobre Aspectos éticos de los implantes TIC en el cuerpo humano, de 16 de marzo de 2005. http://ec.europa.eu/european group ethics/docs/avis20 fr.pdf.

[178] GT29. Documento de 17 de marzo de 2004, sobre datos genéticos.

constitucionales; constituyendo, al mismo tiempo, un vínculo de unión con la política y las instituciones[179].

Respecto a los datos biométricos[180], aunque no tienen la consideración de datos de salud, se asimilan a ellos por el Reglamento, aplicándose las mismas reglas, como las relativas a las causas de legitimación[181].

En cuanto a su contenido, los datos de salud se integran dentro de las categorías especiales de datos personales, constituyendo datos de carácter íntimo que afectan a la dignidad de la persona, estando, además dotados de un gran potencial discriminador que hace que su acceso no autorizado por terceros pueda atentar contra la intimidad personal y familiar; lo que lleva a considerarlos como datos especialmente protegidos, necesitando, para su tratamiento, el consentimiento expreso del interesado[182].

1.2.2. LOS DATOS DE SALUD EN EL RGPD, EN LA LOPDGDD Y EN LA NORMATIVA SECTORIAL DE SALUD: NUEVAS CATEGORÍAS DE DATOS SENSIBLES

Como reconoce el Considerando 52 del RGPD, refiriéndose a las excepciones a la prohibición de tratamiento de estos datos:

" (…) *Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros…. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen*

[179] RODOTÁ, Stefano, "El derecho a tener derechos", Trotta, Madrid, 2014.

[180] Se definen 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", art. 4.14 RGPD.

[181] ÁLVAREZ RIGAUDIAS, C., "Tratamiento de datos de salud", en PIÑAR MAÑAS, J.L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, *op.cit*., pp. 173 y ss.

[182] Considerar las Directrices del GT29 sobre el consentimiento en el sentido del Reglamento 2016/679, adoptadas el 28 de noviembre de 2017.

del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos (…)"

Así pues, en este ámbito nos encontramos, con la interacción y coexistencia necesaria de un derecho fundamental, el derecho a la protección de datos personales, con la necesaria asistencia sanitaria al paciente o interesado. Por ello, a fin de equilibrar los distintos intereses en juego y conseguir tanto la protección procedente de los datos como la necesaria y fundamental prestación asistencial, es preciso compaginar la normativa propia del derecho a la protección de datos (antes vista) con las propias del ámbito sanitario o de la salud: tanto las que regulan el ejercicio de derechos, deberes y garantías de los pacientes o usuarios sanitarios, como las que reglamentan la organización y gestión del sistema sanitario. Así, entre las primeras, habría que considerar cómo interactúan el derecho a la asistencia sanitaria del paciente y su protección de la intimidad con la protección de datos personales, y, por último, el secreto profesional.

Además del ya citado Convenio 108 (cuyo art. 10 proclama el respeto a la vida privada en el ámbito de la salud y el derecho a conocer cualquier dato registrado derivado de su atención sanitaria), y de la CDFUE, que considera derecho fundamental la protección de datos personales y declarando el derecho de toda persona a dicha protección, es preciso referirse por su trascendencia a los Principios Éticos de la Sanidad en la Sociedad de la Información[183], en el que se contienen cuatro principios básicos en el tratamiento de datos de salud:

a) Recogida de los datos, siempre que sea posible del propio interesado (también de los familiares habría que incluir),

b) Control (y disposición) de los datos de salud por el propio interesado;

c) Derecho de oposición de sus datos cuando la finalidad no se corresponda con la de recogida;

[183] Elaborado por el Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías, 30 de julio de 1999.

d) Justificación de la utilización de los datos personales en la proyección social de la salud.

En el ámbito sanitario, la publicación de la LBAP[184], además de su indudable trascendencia, vino a suponer una nueva filosofía en la relación paciente-usuario y los servicios sanitarios, otorgando al paciente más protagonismo en su proceso asistencial al hacerle partícipe y corresponsable de su salud; lo cual se pone de manifiesto en el deber de facilitar los datos sobre su estado de salud, de manera leal y verdadera, además de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o lo requiera la asistencia sanitaria[185].

El derecho a la intimidad e integridad del paciente proclamado como principio básico de la ley se traduce en la necesidad de que el profesional sanitario previo a cualquier actuación sanitaria recabe el consentimiento del paciente.

En el marco de la legislación autonómica, como predecesoras de la LBAP, pueden señalarse, la Ley 21/2000, de 29 de diciembre, de Cataluña, de Derechos de información concernientes a la salud y a la autonomía del paciente y la documentación clínica; la Ley 3/2001, de 28 de mayo, de la Comunidad de Galicia, reguladora del consentimiento informado y de la historia clínica de los pacientes; y la Ley Foral de Navarra 11/2002, de 6 de mayo, sobre los derechos de los pacientes a las voluntades anticipadas, a la información y a la documentación pública. Posteriormente, la mayoría de las Comunidades Autónomas (CCAA) han dictado leyes específicas sobre el derecho a la información y documentación clínica.

Junto a la LBAP y a la LGS[186], podemos encontrarnos con el resto de legislación reguladora en determinados aspectos o sectores de la salud: Ley 16/2003, de 28 de mayo, de Cohesión y calidad del Sistema Nacional de Salud; 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 del medicamento y productos sanitarios; Ley 14/2006, de 26 de mayo, sobre Técnicas de reproducción humana asistida, Ley 14/2007, de 3 de julio, de Investigación Biomédica; Real Decreto 1723/2012, de 28 de diciembre, por el que se regulan las

[184] 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.
[185] Art. 5.2. LBAP.
[186] Ley General de Sanidad, Ley 14/1986, de 25 de abril.

actividades de órganos humanos destinados al trasplante; Real Decreto-ley 9/2014, de 4 de julio, por el que se establecen las normas de calidad y seguridad para la donación, la obtención, la evaluación, el procesamiento, la preservación, el almacenamiento y la distribución de células y tejidos humanos y se aprueban las normas de coordinación y funcionamiento para su uso en humanos; y, por último, las relativas a la salud pública: Ley 33/2011, de 4 de octubre, General de Salud Pública y la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de salud pública.

Habría que destacar la reciente publicación del Real Decreto Ley sobre seguridad digital, que contempla que, en base a "motivos de seguridad pública", los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión de datos de los usuarios del SNS "se ubiquen y presten dentro del territorio de la UE"[187].

Respecto de la normativa específica de protección de datos, por una parte, la LOPDGDD (arts. 8 a 10) contempla tres vías para el tratamiento legítimo de datos personales: "Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos, tratamiento de datos de naturaleza penal y, lo que denomina "categorías especiales de datos", que incluye la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico; para los que el RGPD, en su art. 9, señala como "categoría especial de datos": "(…) datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos, dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, o datos relativos a la vida sexual o las orientación sexuales de una persona física (…)", cuyo tratamiento queda prohibido.

Así, vemos, como el RGPD ha ampliado el contenido de datos especialmente protegidos respecto del configurado por el artículo de la LOPD, incluyendo a los datos genéticos, biométricos y las referencias sobre los datos de origen étnico y de orientación sexual. A ello, habría que añadirse los dos tipos de datos de especial protección regulados en el artículo 15 LTBG[188]; de forma que en el Capítulo III del título II, se abordará el estudio

[187] Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

[188] Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

detallado de estos datos de especial protección, a propósito de su aplicación al ámbito del acceso a la información pública que contenga datos personales.

1.2.3. DERECHO DE LOS PACIENTES A LA CONFIDENCIALIDAD DE SUS DATOS Y OBLIGADO SECRETO DE LOS PROFESIONALES

El principio de confidencialidad constituye un elemento esencial en el tratamiento de la salud y un principio básico de la protección de datos sanitarios, al convertirse la confidencialidad en el elemento que hace que el paciente, en el entorno de la relación de confianza mutua que debe presidir la relación asistencial, suministre al profesional sanitarios datos sanitarios de carácter íntimo. Así, la confidencialidad tiene un ámbito dual: una, la relacionada con el conocimiento de los datos personales del paciente, suponiendo la limitación del acceso a los mismos sólo a personas autorizadas; y otro, a la obligación al personal sanitario y no sanitario que accede a la HC a guardar secreto sobre la información conocida.

Como hemos visto anteriormente, la protección del Derecho va más allá de la intimidad para abarcar la privacidad, término éste más amplio, en el que se incluyen no solamente aspectos íntimos de la persona. Lo íntimo ya no tiene un sentido privativo de lo más interior de nuestra persona, sino que se aproxima al término más activo y extenso de "*privacy*" anglosajón, dotado de una idea de protección de lo particular y de limitación de su acceso a terceros. Así, esta configuración del derecho a la intimidad es la que ha fundamentado la normativa europea y nacional en materia de protección de datos[189].

En el ámbito sanitario, esta protección, se manifiesta a través del derecho de los pacientes –y deber profesional de secreto médico- a la confidencialidad de sus datos médicos –considerados datos sensibles (constituyentes de una categoría especial de datos) que necesitan una especial protección-, además de la cobertura constitucional, y de las leyes. Así, la LGS, que, dentro de los derechos de los usuarios, prevé el respeto a la intimidad y a la confidencialidad de toda la información relacionada con su proceso asistencial[190]; y

[189] En este sentido, ver SUÁREZ RUBIO, M.J., *Constitución y privacidad sanitaria, Op.cit.,* así como la STC 196/2004, de 15 de noviembre, a los que se han hecho alusión anteriormente.
[190] Art. 10.3.

el Convenio de Oviedo de 1997[191], relativo a los derechos humanos y la biomedicina, que proclama el derecho de toda persona a que se respete su vida privada cuando se trate de informaciones relativas a su salud¸ al igual que la LBA [192].

Como instrumento necesario de esta protección, nos encontramos con el secreto profesional sanitario que se traduce en la obligación de guardar el secreto médico y la necesaria confidencialidad de los datos médicos, como derecho y deber fundamental del profesional sanitario en estrecha relación con la confianza depositada por el paciente en dicho profesional[193]; la cual se vería quebrada si esta confidencialidad fuera vulnerada; de ahí, la necesidad de protegerla limitando el acceso a los datos sanitarios exclusivamente a los profesionales sanitarios que intervienen en la asistencia sanitaria del paciente.

Este deber de confidencialidad/secreto médico no afecta sólo a los datos contenidos en la Historia Clínica (HC) sino a todos los derivados del proceso asistencial de paciente con incidencia sanitaria que pudieran identificarse con el titular de los datos. Además, afectará a los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de la actividad sanitaria, y será complementaria a la que están obligados por el secreto profesional; manteniéndose este deber/obligación a pesar de haber finalizado la relación sanitaria[194].

El secreto médico, no obstante, no es absoluto y estaría limitado por las obligaciones impuestas al profesional sanitario en los supuestos de cumplimiento de colaborar con la Administración de Justicia[195], o existencia de riesgo personal o para terceros o que pueda perjudicar la Salud Pública.

---

191 Art. 10.1.

192 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 (art. 7.1)

193 A la necesidad de que el personal sanitario que acceda a la HC guarde el secreto profesional, se refiere el art. 16.6 LBAP.
Así mismo, la Ley 33/2011, de 4 de octubre, General de Salud Pública, prevé el respeto a la dignidad e intimidad personal, así como la obligación de guardar secreto sobre los datos que proporcionen los sistemas de información en el ámbito de la Salud Pública (arts. 7 y 43.2).

194 Art. 5 LOPDGDD, en relación con el deber de confidencialidad previsto en el art. 5.1.f) del RGPD.
Para más información sobre los derechos de los pacientes relacionados con la HC, vide DE LORENZO Y MONTERO, R., *Derechos y obligaciones de los pacientes. Análisis de la Ley 41/2002, de 14 de noviembre, básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica*, Edit. Colex, Madrid, 2003.

195 Obligación de denuncia de cualquier delito que conozca (art. 262 LECrim).

Esta obligación de preservar la información, que se mantendrá aún después de finalizada la relación asistencial, no afecta sólo al personal sanitario, sino también al personal no sanitario que por razón de su trabajo conoce de esa información confidencial[196]. Además de los profesionales sanitarios, en la función asistencial interviene personal que colabora en la gestión administrativa sanitaria que igualmente está obligado a mantener la confidencialidad de la información con la que trabaja; por lo que "todos los usuarios legítimos de datos personales sobre la salud tienen una obligación de confidencialidad equivalente a la obligación profesional del secreto médico"[197]. Y, a esta obligación, que sería complementaria a la de deber de secreto, habría que añadir, como señala el art. 5 de la LOPDGDD, al responsable y encargado del tratamiento, respecto del deber de confidencialidad, previsto en el art. 5.1.f) del RGPD.

El Código Penal[198], castiga la infracción de este deber profesional, a través del delito de revelación de secretos, tipificado en su art. 199; considerando el tipo agravado para cuando sea el profesional el que divulgue los secretos de otra persona, incumpliendo su obligación de sigilo (apartado 2).

El secreto profesional tiene su primera previsión normativa en el texto constitucional (art. 20.1.d), al hablar del derecho a la información, sin que el desarrollo normativo previsto se haya llevado a cabo; por lo que no existe actualmente una regulación concreta del secreto profesional en su contenido amplio. Ello, obliga a acudir a la normativa propia de ámbitos diversos para analógicamente extraer sus consideraciones jurídicas. Así, se considera intromisión ilegítima "la revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela"[199]; y el acceso a los datos sanitarios por persona no autorizada, que incluye tanto a profesionales sanitarios que no tienen relación directa con el paciente, como a otro tipo de personal que presta servicios en la asistencia sanitaria sin vinculación profesional inmediata con el paciente; lo que constituye un acceso indebido o no autorizado, sancionable, incluso penalmente.

196 Art. 2.7. LBAP.

197 Grupo Europeo de Ética de la Ciencia de las Nuevas Tecnologías, *Op.cit.*

198 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, modificado principalmente por Ley Orgánica 1/2015, de 30 de marzo. Otras modificaciones, Ley 2/2019, de 1 de marzo.

199 Art. 7.4 de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

Recordemos, que el art. 72 LOPDGDD considera falta muy grave "La vulneración del deber de confidencialidad establecido en el art. 5 de esta Ley".

No obstante, por ejemplo, el Delegado de Protección de Datos (DPD) podrá tener acceso a los datos de salud, sin que el responsable del tratamiento pueda oponerse alegando la existencia de un deber de confidencialidad (como el del art. 5)[200]. Además, en las medidas técnicas y organizativas que sean más apropiadas a adaptar por el responsable y encargado del tratamiento deberán incluir aquellas que pueden provocar más riesgo para la pérdida de confidencialidad de datos sujetos al secreto profesional[201].

Actualmente, la actividad sanitaria se presta por equipos multiprofesionales en los que cada miembro es responsable del conjunto de la información manejada y, por tanto, todo ellos estarían bajo del deber de respetar la confidencialidad. De forma que esta obligación de preservar la información no afecta sólo al personal sanitario, sino también al personal no sanitario que por razón de su trabajo conoce de esa información confidencial.

Por ello, hay que considerar que en el proceso asistencial del paciente interviene, además, personal administrativo que colabora en la gestión sanitaria, que igualmente está obligado a mantener la confidencialidad de la información con la que trabaja. De esta forma, el secreto médico se convierte en un secreto compartido por todo el personal que trabaja en los Servicios regionales de Salud en funciones asistenciales.

La legislación sanitaria aborda el secreto profesional, en concreto al referirse al acceso a la HC por razones epidemiológicas o de protección de la salud pública, señalando que habrá de realizarse por un profesional sanitario "(…) *sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto* (…)"[202].

[200] Art. 36.3 RGPD.
[201] Art. 28.2.a) RGPD.
[202] Art. 16.2 LBAP.
Para más información sobre la HC, vide CARNICERO GIMÉNEZ DE AZCÁRATE, J., *El derecho a la protección de datos en la historia clínica y la receta electrónica*, Aranzadi, Pamplona, 1999.

En el ámbito profesional, el Código de Deontología Médica, contempla, en el art. 27, los aspectos principales de este deber profesional[203]:

"1.- El secreto médico es uno de los pilares en los que se fundamenta la relación médico-paciente, basada en la mutua confianza, cualquiera que sea la modalidad de su ejercicio profesional.

2.- El secreto comporta para el médico la obligación de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, lo que haya visto y deducido como consecuencia de su trabajo y tenga relación con la salud y la intimidad del paciente, incluyendo el contenido de la historia clínica.

3.- El hecho de ser médico no autoriza a conocer información confidencial de un paciente con el que no se tenga relación profesional".

Por su parte, la legislación sobre protección de datos se refiere al secreto profesional, al tratar las obligaciones del responsable y del encargado del tratamiento, señalando que en la adopción de medidas técnicas y organizativas que adopten para garantizar y acreditar que el tratamiento se realiza conforme al Reglamento, tendrán en cuenta los mayores riesgos que podrían producirse derivados de la "pérdida de confidencialidad de datos sujetos al secreto profesional"[204].

El RGPD, se refiere al deber de secreto y de confidencialidad como "secreto profesional u obligaciones de confidencialidad"; los cuales deberán conciliarse con el derecho a la protección de datos personales (art. 90.1). A fin de hacer efectivo este deber, los hospitales y centros sanitarios deberían establecer normas internas que obliguen a seguir la confidencialidad de los datos a todo el personal (además de estudiantes o personal externo) que pueda tener acceso a los datos de pacientes, que deberán suscribir un compromiso de confidencialidad al inicio del ejercicio de sus funciones.

[203] Código de Deontología Médica de la OMC, de julio de 2011.

[204] Art. 28.2.a) LOPDGDD en relación con los arts. 24 y 25 del RGPD.
Así mismo, el RGPD se refiere a la obligación del delegado de protección de datos de mantener el secreto o la confidencialidad en el desempeño de sus funciones (art. 38.5).
Del mismo modo, este secreto profesional u obligaciones de confidencialidad deberán conciliarse con el derecho a la protección de datos personales (art. 90.1).

A propósito del cumplimiento del deber de secreto, no sólo incumbe a personas físicas relacionadas con los datos del paciente, sino que también los propios centros sanitarios, en la persona de su director o gerente, serían los encargados de dar cumplimiento al mismo, en este caso de forma indirecta. Así, aunque ya en menos centros (quizás más en clínicas privadas), puede observarse como el médico o enfermera para avisar al paciente para que pase al despacho médico le llama por megafonía utilizando su nombre y apellidos, de viva voz y con la sala de espera con otras personas, vulnerando directamente este deber de secreto. Por ello, deberían utilizar medidas que anonimicen la identidad del paciente, preservándolo del resto, como puede ser el empleo de un ticket identificativo con un código numérico, que luego es visionado en una pantalla por el paciente de que se trate la llamada.

1.2.4. DOCUMENTACIÓN CLÍNICO-SANITARIA PORTADORA DE DATOS DE SALUD

Para conocer los documentos que contienen datos personales de salud, hemos de acudir a la definición de "información clínica" que facilita la LBAP: "*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*". Al mismo tiempo, los documentos que contienen los datos de salud se agrupan bajo el concepto de "documentación clínica", considerada como "(…) *el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial*"[205].

La LBAP dedica sus grandes apartados a la información sanitaria y autonomía del paciente (Capítulos II y IV), y a la HC y demás documentación clínica (V y VI). Su entrada en vigor vino a suponer un hito importante al configurar una nueva dimensión del Derecho Sanitario de los derechos y obligaciones de los pacientes, sustentada en una serie de principios puramente deontológicos o de ética médica. Así, dentro de los denominados "principios básicos", el artículo 2 se refiere al respeto y dignidad de la persona humana y su autonomía, que se materializa a través de la exigencia previa del consentimiento del

[205] Art. 3 LBAP.

paciente, una vez informado adecuadamente, y su respeto, a través del derecho a la negación del tratamiento.

La documentación clínica supone el conjunto de información de carácter sanitario sobre un paciente concreto, en la que se incluye la historia clínica (apartado V) y otra documentación, como el informe de alta de paciente y los certificados médicos. Sin embargo, a esta documentación habría que añadir, además de las instrucciones previas (art. 11), otros documentos regulados fuera de la LBAP, como la receta médica y órdenes de dispensación de medicamentos y la tarjeta sanitaria; todos ellos, comprensivos de información/datos de contenido sanitario y, por tanto, necesitados de una especial protección. La historia clínica, será objeto de un estudio independiente y pormenorizado.

1.2.4.1. Documento de voluntades anticipadas

Se denominan de varias formas: testamento vital, voluntades anticipadas, directivas anticipadas. Instrucciones previas es el término empleado por la LBAP[206].

Estamos, por tanto, ante un documento de carácter sanitario, que puede entregarse en un registro público o en el centro hospitalario, derivado de la autonomía prospectiva del paciente, que le permite prolongar esta autonomía cuando su estado de salud le impida adoptar decisiones sanitarias por sí mismo. Este documento incluye, o es susceptible de incluir, datos personales, mediante manifestaciones anticipadas de la persona sobre los cuidados y tratamientos de la salud, para que sean aplicadas cuando no pueda expresarlas.

Estas manifestaciones anticipadas se refieren a[207]: los cuidados y el tratamiento de la salud[208], al destino del cuerpo y los órganos, después de fallecido, y a la posibilidad de designar un representante interlocutor[209].

[206] La denominación legal prevista en el art. 11 LBAP, tiene su origen en el Convenio de Oviedo de 1997, cuyo art. 9, refiriéndose a decisiones anticipadas sobre la salud señala: "Serán tomados en consideración los deseos expresados anteriormente con respecto a una intervención médica por un paciente que, en el momento de la intervención, no se encuentre en situación de expresar su voluntad".

[207] Art. 11 LBAP.

[208] La Ley del País Vasco, de 12 de diciembre de 2002, indica que las Instrucciones Previas pueden referirse tanto a una enfermedad o lesión que ya padece el otorgante como a las futuras.

[209] Parece aconsejable desde el punto de vista clínico al proporcionar una mayor certeza de la voluntad del enfermo y su adecuación a la situación presente.

Un problema real que plantean las instrucciones previas se basa en su carácter de documento no ajustado a la realidad del momento en que tienen que aplicarse, en el que la situación personal del paciente y del estado de la ciencia pueden no ser las previstas inicialmente. Por ello, ante el problema de su aplicabilidad por el profesional sanitario, MONTALVO JÄÄSKELÄINEN[210], entiende que la solución debe venir por la aplicación del criterio de la irreparabilidad de la situación del paciente; de forma que, únicamente serán vinculantes en el ámbito o en el contexto de la fase terminal o del final de la vida. Otros autores, como DOMINGUEZ LUELMO, entienden necesario que su elaboración sea suficientemente amplia y dinámica, que permita su posterior adaptación a la realidad futura[211].

Junto al Registro Nacional de Instrucciones Previas, todas las CCAA han dictado leyes sobre el derecho a formular instrucciones previas[212] y han regulado sus propios registros conectados con el nacional; cuya información constituye ficheros a los efectos de la normativa de protección de datos personales, en los que se inscriben las voluntades anticipadas de las personas mediante documentación suscrita por el interesado, así como sus modificaciones o revocación. Así, esta información se pone a disposición del personal sanitario de los centros sanitarios, que tiene obligación de conocerla y aplicarla en el momento que proceda.

[210] MONTALVO JÄÄSKELÄINEN, F., "*Límites a la autonomía de voluntad e instrucciones previas: un análisis desde el derecho constitucional*",Vol. 20, nº 1, 2010,V/Lex, pp. 121-162.
www.Dialnet-LimitesALaAutonomiaDeVoluntadEInstruccionesPrevias.

[211] DOMÍNGUEZ LUELMO, A., "Derecho sanitario y responsabilidad médica. Comentarios a la Ley 41/2002, de 14 de noviembre, básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica", Edit. Lex Nova, 2ª edic., Valladolid, 2007.

[212] Por ejemplo, la Comunidad de Madrid ha dictado la Ley 3/2005, de 23 de mayo, por la que se regula el ejercicio del derecho a formular instrucciones previas en el ámbito sanitario y se crea el registro correspondiente. "Las instrucciones sobre el tratamiento pueden incluir previsiones relativas a las intervenciones médicas que se deseen recibir, aquellas que no se deseen recibir u otras cuestiones relacionadas con el final de la vida, siempre que sean conformes con la *lex artis"* (art. 6.2).
Para más información, vide SÁNCHEZ GÓNZALEZ, I., "Informe sobre instrucciones previas", MARTÍN SÁNCHEZ. I., (coord.), Consejería de Sanidad, Comunidad de Madrid, 2005.

1.2.4.2. Recetas médicas y Órdenes de dispensación: sus implicaciones en materia de protección de datos

La receta médica es el documento normalizado utilizado por los profesionales sanitarios legalmente habilitados, destinado a la prescripción de medicamentos o productos sanitarios para su dispensación a los pacientes. Este documento sanitario se encuentra regulado en el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, en cuyo art. 3 se contiene la definición de receta médica[213], junto a la de "orden de dispensación hospitalaria", para pacientes no ingresados, y la orden de dispensación, por la que los enfermeros acreditados indican o autorizan los medicamentos sujetos a prescripción médica. Estos documentos, como forma de instaurar un tratamiento, únicamente pueden ser emitidos por un médico, odontólogo o podólogo, como profesionales exclusivos en la receta de medicamentos sujetos a prescripción médica[214].

La receta y la orden de dispensación, como documentos sanitarios en los que se refleja un aspecto (a través de los medicamentos dispensados) del tratamiento sanitario, deben contener los datos básicos de identificación de prescriptor, paciente y medicamentos[215], lo que implícitamente conlleva información de la salud del mismo; por tanto, conteniendo datos personales sensibles, de especial protección.

Así, la ley[216], cuyo título precisamente se denomina "Protección de datos en las recetas médicas y órdenes de dispensación hospitalarias", establece que en la tramitación de las recetas y órdenes de dispensación y, sobre todo, en su tratamiento informático "(…) *deberá quedar garantizada, conforme previene la normativa específica de aplicación, la*

[213] "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".

[214] 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. Al mismo tiempo, El 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, ha venido a regular la llamada "prescripción enfermera", por el que los enfermeros acreditados podrán indicar y autorizar la dispensación de determinados medicamentos sujetos a prescripción médica en base a protocolos y guías de práctica clínica y asistencial.

[215] Art. 79.4 RDLeg.1/2015, de 24 de julio.

[216] Art. 19 del Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.

confidencialidad de la asistencia médica y farmacéutica, la intimidad personal y familiar de los ciudadanos y la protección de sus datos de carácter personal".

Esta confidencialidad, junto a su seguridad y adecuada conservación, deberán garantizarse por el farmacéutico una vez sean dispensadas las recetas médicas en papel[217].

La Disposición adicional séptima del Real Decreto, se denomina "Tratamiento de la información", y señala que para las actuaciones previstas en el mismo que tengan relación con el tratamiento, cesión y custodia de datos de carácter personal se estará a lo previsto en la LOPD y su Reglamento.

1.2.4.3. Receta electrónica

Se trata de una modalidad de servicio digital utilizada como apoyo a la asistencia sanitaria, a través de la cual la prescripción de medicamentos y productos sanitarios que luego serán dispensados al paciente se realiza mediante medios electrónicos dentro del contexto de las TICs.

Los ficheros que contienen datos personales de salud derivados de la receta médica en papel o en formato electrónico, para su tratamiento no necesitan del consentimiento de la persona afectada[218] y, del mismo modo, el tratamiento de datos por parte de las Entidades gestoras de la Seguridad Social no requiere el consentimiento del titular de los datos[219].

[217] Art. 19.1 del Real Decreto 1718/2010, de 17 de diciembre, en relación con el art. 6 RGPD y LOGDPDD, Disp. Adic. 17ª.

[218] Arts. 79.8 y 103 RDLeg.1/2015, de 24 de julio.
En el mismo sentido, art. 19.2 RD. 1718/2010, de 17de diciembre, que establece:
"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 los artículos 7, apartados 3 y 6; 8; y 11, apartado 2.a), de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. 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, incluidos los distintos regímenes especiales de las Mutualidades de Funcionarios".

[219] De acuerdo con el informe de la AEPD 126/03, las actuaciones que prevé el concierto entre las Oficinas de farmacia con el SNS y cada Comunidad Autónoma para que sean los Colegios Oficiales de Farmacéuticos los que asuman las funciones de colaboración, señala que las actuaciones que el concierto exige de los Colegios Profesionales en relación al tratamiento automatizado de datos personales contenidos en las recetas, constituyen un supuesto de cesión de datos entre Administraciones públicas (art. 21 LOPD).

A nivel europeo, tendremos ocasión de tratar la receta electrónica en el apartado de a asistencia sanitaria transfronteriza. En el ámbito nacional, está muy avanzada la receta electrónica interoperable, lo que permitirá realizar cualquier dispensación farmacéutica en cualquier parte del territorio.

El art. 19 del Real Decreto 1718/2010 se refiere a la protección de datos de las recetas y órdenes de dispensación, señalando que (especialmente en el tratamiento informático) deberá quedar garantizada la confidencialidad de la asistencia sanita y farmacéutica, con el fin de proteger el derecho a la intimidad de los pacientes y protección de datos de los pacientes.

En las recetas médicas en soporte papel y en la hoja de información al paciente que se entrega con la receta electrónica se incluirá una cláusula que informe al paciente, en los términos establecidos en el art. 5 LOPD, para dar cumplimiento al principio de información[220].

Sobre la seguridad de los datos contenidos en la receta electrónica, el art. 11 del Real Decreto señala:

"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, de conformidad con lo dispuesto en la LOPD, para lo que se implantarán medidas de seguridad de nivel alto".

"Para garantizar dichos niveles de seguridad, esta información sólo será accesible desde la oficina de farmacia a efectos de dispensación, residirá de forma permanente en los sistemas de receta electrónica gestionados por las Administraciones sanitarias y no podrá ser almacenada en los repositorios o servidores ajenos a éstas, establecidos para efectuar la facturación, una vez esta se haya producido".

Los datos necesarios para la prescripción médica y su acceso son responsabilidad del prescriptor, que además conservará los impresos y talonarios de recetas médicas (art. 18.1); aunque para las Mutualidades de funcionarios la responsabilidad de conservación

[220] Art. 3 RD 1718/2010 de 17 de diciembre.

y custodia corresponde a los beneficiarios. Tratándose de recetas electrónicas del SNS el farmacéutico se responsabilizará del acceso a los datos disponibles a fin de procurar la dispensación en su oficina de farmacia (art. 18.4).

1.3. PROTECCIÓN DE DATOS EN LA INVESTIGACIÓN BIOMÉDICA

1.3.1. PROTECCIÓN DE LA INTIMIDAD EN LOS PROYECTOS DE INVESTIGACIÓN

Uno de los lugares más importantes para la investigación son los hospitales, en los que se lleva a cabo distintos tipos de investigación sanitaria: a) tanto la investigación básica, que, alejada de una aplicación práctica, se centra en un mejor conocimiento del proceso salud-enfermedad, sin que sea necesario el acceso a datos personales de pacientes; b) como la investigación clínica, dirigida a mejorar el diagnóstico, tratamiento y prevención de enfermedades en las personas, que puede requerir el acceso a datos personales de los pacientes o de los voluntarios sometidos al estudio, y se realiza mediante ensayos clínicos, que normalmente se centran en medicamentos aunque pueden realizarse sobre productos sanitarios, y llevan aparejado un tratamiento de datos de salud de las personas participantes en el estudio. Centrado más en el aspecto académico o educativo, encontramos los estudios retrospectivos, como tesis doctorales, o proyectos de fin de grado; pudiendo existir el acceso a la HC de pacientes vinculados a un hospital o centro sanitario, en cuyo caso, habrían de aplicarse medidas de protección de los datos sanitarios incluidos en la misma.

En un proyecto de investigación, la propiedad de los datos derivados de la investigación pertenece al promotor[221] del estudio del ensayo clínico, sin posibilidad de acceso a los datos de identificación de los participantes en el mismo; de forma que la recogida de datos y las comunicaciones de resultados de la investigación se recogen en repositorios de datos disociados, en los que no hay identificación del paciente[222].

[221] Supone la figura impulsora económicamente del proyecto, generalmente empresas farmacéuticas.

[222] Para más información sobre la propiedad de los datos personales, ver el artículo de HERNÁNDEZ CORCHETE, J.A., "La propiedad de los datos personales. ¿Los datos como moneda de cambio?", *El Cronista del Estado Social y Democrático de Derecho*, n.º 88-89, 2020.

Normalmente las investigaciones con un grado de reconocimiento público siguen un protocolo previo, en el que uno de sus apartados son las pautas a seguir para el tratamiento de datos personales de los sujetos implicados en el estudio. Además, el proceso de investigación esta supervisado normalmente por un Comité Ético de investigación médica, que es el encargado de velar por el respeto de la legislación de protección de datos.

Los ensayos clínicos realizados son incluidos dentro de la HC de cada paciente existente en el Sistema de Información del hospital, dada su posible utilidad a efectos asistenciales del paciente; pudiendo acceder a dicha HC únicamente el personal sanitario autorizado.

Sólo el investigador principal, como responsable del proyecto, así como sus colaboradores, si fueran autorizados, conocen los datos identificativos de las personas que participan en el ensayo clínico.

El RGPD se refiere al tratamiento de datos personales con fines de investigación científica, señalando que ésta debe interpretarse de manera amplia, de forma que,

"(…) *incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública".*

"Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas".

1.3.2. MEDIDAS PARA EVITAR LA IDENTIFICACIÓN DEL INTERESADO

En el apartado 2.2., al tratar de la HC, nos hemos referido a la necesidad de disociación de los datos identificativos de la personalidad del paciente de los puramente clínicos o asistenciales en procesos de investigación científica.

El RGPD establece una base de legitimación para proceder a la investigación científica que está unida a dos principios:

a) la previa existencia de una ley, como es la Ley 14/2007 de Investigación Biomédica, que añada otras causas de legitimación distintas del consentimiento;

y, b) la necesidad de que existan garantías adecuadas para los derechos y libertades de los interesados, a través de medidas técnicas y organizativas que respeten el principio de minimización de datos, y que "(…) *podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines (…) mediante un tratamiento ulterior que no permita o ya no permita la identificación del interesado*"[223].

Además, tanto el Derecho de la Unión como de los Estados miembros, podrán 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*"[224].

Por tanto, las salvaguardas de protección de los derechos y libertades de los interesados consisten en la aplicación de medidas técnicas y organizativas, como la aplicación del principio de minimización de datos y la seudonimización. Sobre el primero, como señala ÁLVAREZ RIGAUDIAS[225], llama la atención el que tratándose de un ámbito como el de la investigación en que por su propia filosofía y contenido debe basarse en un contenido amplio casi totalmente abierto a lo que pueda resultar del proceso investigador, el hecho de que se apliquen técnicas de anonimización que "mantengan el valor científico del dato (lo que excluye en muchos casos la completa e irreversible anonimización) y la protección

[223] ALVAREZ RIGAUDIAS, *op. cit*., pp. 177-181.
[224] Art. V89 y Considerando 156 RGPD.
[225] EL EMAM K, ÁLVAREZ C. "A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techiques*",* In *Data Privacy Law*, 2015, pp. 179-180,

de la confidencialidad del paciente, puedan limitar este carácter abierto y prácticamente ilimitado que debe tener la investigación". No obstante, podría entenderse que se reduce esa limitación al compatibilizarse con la posibilidad que prevé el propio art. 5.1.e) del RGPD, de mantenimiento de los datos personales con fines de investigación científica por períodos más largos que el que, como principio general, establece el tiempo necesario para el cumplimiento de los fines del tratamiento.

Otra de las técnicas a utilizar sería la seudonimización, como técnica parcial de anonimización de datos, y al mismo tiempo como medida de seguridad, que consiste en

"(…) *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"*[226].

Después del tratamiento de seudonimización los datos personales, salvo que exista una definición clara y vinculante de "datos seudonimizados" distinta de los de "datos personales"[227] siguen siendo considerados datos personales: "Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable[228]". Por ello, entiendo que la seudonimización supone la mejor técnica o medida para proteger los datos personales utilizados en el contexto de la investigación científica, en concreto la referida al ámbito biomédico.

[226] Art.4. RGPD.

[227] Dictamen 3/2015, de 28 de julio, del Supervisor Europeo de Protección de Datos.

[228] "Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos" (Considerando 26 RGPD).

2. TRATAMIENTO Y CESIÓN DE DATOS DE SALUD

2.1. PRINCIPIOS APLICABLES AL TRATAMIENTO DE LOS DATOS DE SALUD

Como señala ARIAS POU, el Reglamento, define, al igual que la Directiva 95/46, el tratamiento como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, utilizando o no procedimientos automatizados, viniendo a incluir en estos supuestos la estructuración y la adaptación, además de sustituir la referencia al bloqueo por la limitación, como nueva definición, en la que se alude al marcado de los datos personales conservados a fin de limitar su conservación[229].

Los principios de protección de datos fueron por primera vez reconocidos mediante el Convenio 108, el cual tiene por objeto garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. En el Convenio, bajo la perspectiva de "calidad de los datos", se reconocieron los principios de calidad de datos, categorías particulares de datos, seguridad de los datos y demás garantías complementarias para la persona concernida.

Por su parte, a escala mundial fueron las Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE), las que adoptaron una variedad de principios comunes referidos a la protección de datos personales[230]. La OCDE creó en sus Directrices los siguientes principios:

- Principio de limitación de recogida según el cual se limita la recopilación de datos personales, además de instar a que dichos datos deban ser recogidos legalmente e incluyendo el conocimiento o consentimiento interesado.

- Principio de calidad de los datos según el cual éstos deberán ser relevantes para la intención de uso, pero además deberán ser exactos, completos y actuales.

[229] ARIAS POU, María, "Definiciones a efectos del Reglamento general de protección de datos", en *Reglamento General de protección de datos* …, p. 120.

[230] Directrices para la Protección de la intimidad y de la circulación transfronteriza de datos personales. (23 de septiembre de 1980). Organización para la Cooperación y el Desarrollo Económico. París.

- Principio de delimitación de uso, del cual se infiere que no se podrá divulgar o usar los datos personales para propósitos distintos a los informados para su recopilación. Este principio establece una excepción cuando el consentimiento es dado por el interesado o por una imposición legal.

Otros principios:

- Principio de especificación del propósito, según el cual éste se deberá especificar al momento de la recogida;
- Principio de salvaguardia de la seguridad empleando mecanismos razonables para mitigar los riesgos;
- Principio de transparencia, implementando políticas relativas a verificar la naturaleza y existencia de datos personales, así como el propósito de su uso;
- Principio de participación individual que da derecho al interesado a ser informado cuando un controlador de datos posee los suyos;
- -y el Principio de responsabilidad del cumplimiento de los principios generales.

Estas directrices supusieron un punto de partida, conforme al cual los principios generales de la protección de datos fueron cristalizando la "*opinio iuris*" generada a lo largo de dos décadas y definiendo derechos y garantías encaminadas a asegurar la observancia de dichos principios recogidos en dicho instrumento[231].

En esa misma línea, en sus considerandos, la Directiva 95/46/CE indicaba los principios de protección de datos, expresando que la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en dicha Directiva, precisan y amplían los del Convenio 108[232].

Además, expresa dicha Directiva que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario; además, debe excluirse el tratamiento de datos efectuado por una persona física en el ejercicio de

[231] DEL PESO NAVARRO, E., *Ley de Protección de Datos: la nueva LORTAD*, Díaz de Santos, Madrid, 2000, p. 17.
[232] Considerando 11 RGPD.

actividades exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones[233].

En ese sentido, los principios propuestos por la Directiva 95/46/CE se dividen en dos: los referidos a la calidad de los datos; y los referidos a la legitimación del tratamiento. Además, promueve otros, referentes según las categorías especiales de tratamiento: a la información a los afectados por dicho tratamiento, al derecho de acceso del interesado a los datos, a las excepciones y limitaciones, al derecho del interesado a oponerse al tratamiento, la confidencialidad y la seguridad del tratamiento y la notificación del tratamiento a la autoridad de control.

No obstante, más allá de las distintas clasificaciones aportadas por las múltiples normativas, lo cierto es que la mayor parte de la doctrina coincide en una clasificación fundamental de los principios generales de la protección de datos. En ese sentido, se encuentran los principios de calidad, principio de información y el principio de seguridad de los datos.

Después de aprobado el RGPD, se mantiene inalterada la especial importancia que tienen estos principios, por su efecto expansivo sobre todo el ordenamiento de la protección de datos, sobre el que se refleja su carácter informador, "debiendo aplicarse a toda información relativa a una persona física identificada o identificable"[234]; por lo que puede afirmarse que constituyen el contenido esencial del derecho a la protección de datos, configurándose a través de ellos un sistema de tutela que se traduce en una utilización más racional y razonable de los datos personales[235]. Además, la redacción utilizada por el Reglamento para su regulación tiene básicamente carácter continuista, tanto de la Directiva 95/46, como de la LOPDGDD[236].

[233] Considerando 12 RGPD.
[234] Exposición de Motivos del RGPD.
[235] HERRAN ORTIZ, A, "El derecho a la protección de datos personales en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos*, nº 26, Universidad de Deusto, 2003.
[236] PIÑAR MAÑAS, J.L., Jornadas ENATIC sobre "El nuevo Reglamento Comunitario de Protección de Datos", CGAE, Madrid, 29-4-2016

Para MURILLO DE LA CUEVA y PIÑAR MAÑAS, se destacan los principios de: consentimiento, información, finalidad, calidad de los datos, proporcionalidad y seguridad, establecidos en la LOPD[237].

2.1.1. PRINCIPIO DE CALIDAD DE LOS DATOS

Este principio puede calificarse como esencial dentro del engranaje del sistema de protección de datos. La LOPD se refería al principio de calidad de los datos como la garantía de adecuación, exactitud, pertinencia y proporcionalidad de los datos de carácter personal, obligando al responsable del tratamiento a su cumplimiento. Así, los datos han de ser pertinentes y adecuados a la finalidad perseguida, utilizándose exclusivamente los datos necesarios para la finalidad solicitada. Por ello, un dato es adecuado, pertinente y no excesivo cuando su recogida y tratamiento guarda relación con el fin determinado para el que se ha obtenido.

El principio de calidad es susceptible de aglutinar a su vez otros principios: proporcionalidad, finalidad, exactitud y actualidad, cancelación de oficio, licitud y lealtad.

i) Proporcionalidad

Este principio está íntimamente unido al principio de pertinencia, por el que sólo deber procederse a la recogida y tratamiento de aquellos datos que sean adecuados, pertinentes y no excesivos en función de las facultades para las que se hayan obtenido. A estos condicionantes exigidos por la LOPD y su reglamento, el RGPD añade la necesidad de que el tratamiento sea lícito, leal y transparente.

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[238]. Por su

[237] MURILLO DE LA CUEVA, P.L. y PIÑAR MAÑAS, J.L., "El Derecho a la autodeterminación Informativa". *op.cit.*, p. 101.
[238] Considerando 4, RGPD.

parte la LOPDGDD se refiere a los principios de proporcionalidad e intervención mínima en su art. 89.3, al referirse a uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

La aplicación de este principio se traduce en la existencia de distintas finalidades que persigue el tratamiento y los datos que se manejan; de forma que debe articularse un equilibrio entre ambos que permita que se proceda al tratamiento de los datos de forma coherente y relacionado con la finalidad perseguida, que, tratándose de datos sanitarios, sería la protección de la salud de la persona.

De esta forma, si la medida restrictiva del derecho resulta desproporcionada no estará justificada la legitimidad del fin perseguido. Sólo resulta proporcionada si no existen otras medidas menos gravosas que con el menor sacrificio del derecho a la intimidad puedan ser igualmente válidas para conseguir el fin perseguido, o cuando la medida sea más beneficiosa para el interés general que perjuicios para otros bienes o valores[239].

Ya hemos visto en el capítulo 2.2.2. como en el acceso a los datos de salud y, en concreto, en la Historia clínica resulta absolutamente imprescindible respetar este principio, de forma que se limite su acceso a los datos estrictamente necesarios para el cumplimiento de la función asistencial, no sólo por los profesionales sanitarios que intervienen en la asistencia del paciente[240], sino que incluso el acceso por el poder judicial a la Historia clínica debe solicitarse únicamente aquellos aspectos de la HC exclusivamente relacionados con las actuaciones judiciales y no otros o su integridad, como frecuentemente ocurre. Además, el tratamiento de los datos debe responder con la finalidad legítima para la que fueron recabados.

ii) Finalidad

Conforme al art. 4 LOPD y el art. 8 RLOPD, e indirectamente según el art. 94.2 LOPDGG, los datos de carácter personal sólo podrán ser recogidos para el cumplimiento

[239] LÓPEZ ULLA, J.M., "Principios de la protección de datos: datos especialmente protegidos", en *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*, *op.cit*., pp. 7-8.

[240] Sin que pueda extenderse a otros profesionales sanitarios que no tengan tal vinculación (art. 4.1 LOPD).

de finalidades determinadas, explícitas y legítimas del responsable del tratamiento, y estas finalidades son sólo aquellas "para las que se hayan obtenido los datos".

Este principio se encontraba establecido en la derogada LOPD, e indicaba que "*Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos*"[241]. Así, las finalidades incompatibles o no, se determinan por el hecho de que el interesado pueda conocer que los datos autorizados serán usados para un tratamiento y fines para los cuales dichos datos han sido recabados. Y esta incompatibilidad habría que entenderla en el sentido de que:

> *"(...) para un fin incompatible con el derivado del interés apreciado para acceder al Registro, debiendo recordarse que la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, ha venido a sentar la doctrina de que el término "incompatible" debe ser interpretado restrictivamente, debiendo considerarse, con carácter general, asimilado a "distinto"*[242].

Mientras que la LOPDGDD establece que, tratándose del consentimiento que contiene múltiples finalidades será necesario expresar el consentimiento para cada una de ellas, el RGPD lo reconduce más en cuanto a la recogida de datos, indicando que los datos personales serán "(…) *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 (limitación de la finalidad)"*[243], no permitiéndose la identificación de su titular nada más que por el tiempo necesario, salvo las excepciones determinadas por el art. 4.5. LOPD.

[241] Art. 4.2. LOPD.
[242] SAN de 8 de febrero de 2006.
[243] Art. 5.1. RGPD.

Realmente, las consideraciones jurídicas referidas, no indican una definición del principio, sin embargo, se puede interpretar que se refiere a la finalidad como objetivo final que busca la manipulación de los datos.

En este sentido, el consentimiento dado para que nuestros datos se utilicen en una investigación científica (como pueda ser sobre el cáncer de mama) podrá ser utilizado para otras investigaciones que se realicen sobre el cáncer, sin que por tanto exista incompatibilidad entre el primer tratamiento y los posteriores que se realicen.

Siguiendo con el ámbito sanitario de la investigación biomédica, ésta se basa en dos principios de protección de los datos de material biológico del paciente (normalmente), íntimamente conectados entre sí: el de consentimiento informado del sujeto activo y el principio de finalidad, por el que este material biológico únicamente puede ser tratado en la actividad investigadora para aquella finalidad específica para la que el paciente hubiera prestado el consentimiento (normalmente ensayos clínicos). Sin embargo, pueden existir otros usos o utilidades (secundarios) que no respetan esa finalidad, por cuanto se destinan a otros usos distintos a los previstos inicialmente. Estas utilidades, se consideran legales en la medida en que se adaptan a las prescripciones legales establecidas, que promueven una flexibilidad del principio finalista, permitiendo estos usos secundarios cuando el tratamiento de muestras se realiza en un biobanco de investigación[244].

Así, la finalidad se refiere a los motivos en que se fundamenta la utilización de los datos por parte del que será el responsable del fichero, a la actividad a la que dirige dicho responsable la manipulación de la información[245].

Parte de la doctrina considera que se le ha dado una especial relevancia en las normas que regulan la protección de datos de carácter personal al principio de finalidad, aun cuando casi todos los demás principios son considerados fundamentales, ya que tiene presencia no solo en le recogida de datos sino también en su tratamiento[246]. Para PÉREZ VELASCO

[244] GÓMEZ-SALVAGO SÁNCHEZ, *Principio de finalidad y usos secundarios del material biológico de origen humano en la actividad investigadora,* Asociación de juristas de la salud, http://www.ajs.es/sites/default/files/2020-05/vol25n2_05_Estudio.pdf

[245] APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Pamplona, 2000, p.81.

[246] GUICHOT REINA, E., "Datos personales y Administración Pública", *Op.cit.*, p.230-231; SANZ CALVO, L. y LESMES SERRANO, C., *Calidad de los datos; La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*, Lex Nova, Valladolid, 2008, p.146.

la finalidad es de tal importancia que el principio de la finalidad alcanza la mayor relevancia, pues se convierte en la principal garantía para el titular de los datos de que el tratamiento se va a realizar respetando sus derechos fundamentales[247].

iii) Exactitud y veracidad

Así, los datos habrán de ser exactos y actualizados o puestos al día con la finalidad de que se adecuen a la realidad de la persona a la que afectan. A ellos se refería el art. 4.3. LOPD dentro del principio de calidad de los datos. Además, han de ser exactos y puestos al día en relación con la situación actual del afectado; obligación que ha de cumplir el responsable del fichero y que enlaza con la necesaria actividad del interesado de ejercicio de su derecho de rectificación solicitando la modificando los datos iniciales.

Para ello, se adoptarán todas las medidas razonables para que se supriman o rectifiquen los datos personales que sean inexactos con respecto a los fines para los que se tratan; debiendo cancelarse o completarse de oficio si no son auténticos, exactos, veraces y actualizados[248].

La exactitud de este principio conlleva que los datos de carácter personal objeto de tratamiento deben ser precisos y que respondan con la mayor veracidad a la situación que presente el interesado. Esta norma de exactitud trasladada al ámbito sanitario adquiere gran protagonismo, habida cuenta de la importancia que para el proceso de salud del paciente supone que el profesional sanitario trabaje con datos certeros reveladores de un determinado estado salud, pudiendo ser determinantes en la evolución o tratamiento del paciente. Así tiene especial trascendencia esta necesidad del responsable del tratamiento de que la información que figure en la HC del paciente sea veraz, adecuada a la realidad y esté actualizada; por cuanto la prestación de la asistencia sanitaria al paciente se apoya en los datos sanitarios que figuran en la HC, que incluso pueden haber sido incluidos -es lo normal- por otro profesional sanitario.

[247] PÉREZ VELASCO, M.M., *Los Ficheros Públicos, Estudios sobre Administraciones Públicas y Protección de Datos Personales*, "Encuentro entre Agencias Autonómicas de Protección de Datos Personales*".* Thomson-Civitas y APDCM, Madrid, 2006, pp. 4 y ss.
[248] SAN de 23 de marzo de 2016.

Ya hemos visto al hablar del acceso a la HC de la necesidad de que los datos sanitarios se mantengan en buen estado, como estipula la LBAP en sus arts. 14 a 19. Para dicha finalidad resulta fundamental el cumplimiento por parte del paciente de su deber de aportar al profesional sanitario datos ciertos y verdaderos sobre su estado de salud, al margen de las obligaciones de aquel de rectificar, cancelar o sustituir los datos incompletos o inexactos; lo que, en el caso de no conocerse la lengua, podría dar lugar a la necesidad de acudir a un intérprete (obligado también a guardar secreto) a fin de evitar una perjudicial comprensión errónea de los datos transmitidos por el paciente al profesional médico.

Para la AEPD *"*La obligación establecida en el artículo 4 transcrito, impone la necesidad de que los datos personales que se recojan en cualquier fichero sean exactos y respondan, en todo momento, a la situación actual de los afectados, siendo los responsables de los ficheros quienes responden del cumplimiento de esta obligación*"*[249].

iv) Cancelación

Como decíamos, los datos han de mantenerse actualizados, exactos y veraces, por lo que deben cancelarse si ya no son necesarios o pertinentes para la finalidad para la cual han sido registrados (art. 4.5. LOPD). El resultado de la cancelación sería el bloqueo de los datos o su disociación y su supresión, una vez cumplidos los plazos legales.

Centrándonos en el ámbito sanitario, este principio de la protección de datos debe ceder ante los intereses superiores de la atención sanitaria recogidas en la legislación sanitaria, que prevé especificidades resultantes de las necesidades de la atención sanitaria, como pueda ser el plazo de conservación de la HC de cinco años, o más en ciertas leyes autonómicas.

[249] AEPD, Resolución de 31 de mayo de 2005.

2.1.2. PRINCIPIO DE TRANSPARENCIA

Otro principio de importancia capital en la protección de datos, recogido por la derogada LOPD, es el principio de transparencia según el cual el interesado debe ser informado de quien recoge sus datos, quien los tratará y para que fines; constituyendo el fundamento para el ejercicio de otros, como el principio de consentimiento del afectado, siendo así un requisito previo para su emisión. El origen de este principio viene de la Directiva 95/46, que contempla la información respecto de los datos obtenidos del propio interesado. A este respecto el TC, en una sentencia examinada en el capítulo anterior, se refería a que el poder de control que por mor de la protección de datos se atribuye a su titular, sólo es posible y efectivo imponiendo a terceros determinados deberes de hacer,

> *(…) A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos" (FJ 5)*[250].

Se considera este principio como parte del derecho a la autodeterminación informativa, por cuanto al expresar que el derecho del titular de unos datos de carácter personal a ser informado sobre los aspectos que van a definir el tratamiento o la manipulación de los mismos se erige en facultad de extraordinaria relevancia para la salvaguarda del derecho a la autodeterminación informativa[251.]

Sin embargo, el principio de información también conlleva ciertos límites y obligaciones. Así, los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco. No obstante, no solo constituye un deber de información, sino que, como contrapartida, representa un derecho de toda persona a estar en conocimiento de la forma y modos en que se va a desarrollar el tratamiento de datos que le afectan. La desplazada LOPD lo recogía así:

[250] STC 292/2000, de 30 de noviembre.
[251] MARTÍNEZ MARTÍNEZ, R., *Tecnologías de la Información, Policía y constitución,* Tirant lo Blanch, Valencia, 2001, pp. 203-203.

*"Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante" (*art. 5.1).

Sin embargo, se excepciona la obligación de informar: *"(…) cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados…", o cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial*" (art. 5.5.)

No obstante, esta información no será necesario prestarla: "(…) *si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban"* (art. 5.3.).

Por su parte, el RGPD, aun cuando se dispone dicho principio en el Capítulo III referido a los derechos de los interesados, de la lectura del artículo 13 se puede desprender fácilmente que, el principio de transparencia, además de un principio fundamental para la protección de datos, también es una obligación del responsable la recogida de los datos. Así, el RGPD[252], establece que, salvo que el interesado ya disponga de esa información, el responsable del tratamiento estará obligado a:

a) Que en el momento en que se obtengan sus datos personales le facilite toda la información contenida en el artículo 13, apartado 1;

b) Facilitar al interesado, la información necesaria para garantizar un tratamiento leal y transparente, contenida en el apartado 2;

c) "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

[252] Art. 13 RGPD.

interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2" (apartado 3).

En cuanto a la LOPDGDD[253], pareciera contradecirse al expresar que cuando los datos personales sean obtenidos del afectado el responsable del tratamiento *podrá* dar cumplimiento al deber de información. No se entiende realmente si es facultativo o realmente es un deber de información, lo cierto es que por tratarse de un principio se asume que es un deber del responsable del tratamiento. Así, la ley distingue entre:

1) Si los datos personales se han obtenido del afectado, el responsable del tratamiento "podrá dar cumplimiento al deber de información establecido en el artículo 13 del RGPD, facilitándole la siguiente información: 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".

2) 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 facilitando a aquel la información básica señalada en el apartado anterior, e incluirá también las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos".

El GT 29 se refiere a la llamada confidencialidad de una obligación de secreto, con una aplicación fundamental a los profesionales sanitarios y al secreto médico inherente a su profesión, en base al art. 14.5.d) RGPD, que establece una exención al requisito de información del responsable del tratamiento en el caso de que 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". Por tanto, el profesional sanitario se ve afectado directamente por el secreto profesional y, por tanto, no puede facilitar (salvo infracción legal) la información prevista en el art.14, apartados 1,2 y 4 del Reglamento[254].

[253] Art. 11 LOPDGDD.

[254] GT 29, Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, Adoptadas el 29 de noviembre de 2017 Revisadas por última vez y adoptadas el 11 de abril de 2018.
Así, estas directrices contienen el siguiente ejemplo aplicado a la profesión médica: "Un profesional de la medicina (responsable del tratamiento) está sujeto a la obligación de secreto profesional respecto de la información médica de sus pacientes. Una paciente (respecto al cual se aplica la obligación de secreto

2.1.3. PRINCIPIO DE CONSENTIMIENTO

El principio de consentimiento, íntimamente relacionado con el derecho a la autodeterminación informativa, es la principal facultad de control que tiene la persona sobre sus datos, dándole capacidad al interesado para autorizar o no el tratamiento de sus datos.

Se trata de un mandato capital del ordenamiento jurídico que ordena que, para operar con datos personales, obligatoriamente hace falta la aprobación del interesado. Es una libertad del individuo el cual tiene la facultad de decidir como disponer libremente de sus datos, reconociéndose así la capacidad de decidir de un área de su vida personalísima que le pertenece.

La doctrina considera el consentimiento como uno de los pilares fundamentales en el sistema de protección de datos. Así, el consentimiento del afectado es la piedra angular a partir de la cual se construye el sistema de protección de datos personales frente al uso de la informática "la exigencia del consentimiento informado del afectado como regla que ha de observarse antes de proceder a un tratamiento de este tipo de datos. Consentimiento que solamente puede ser obviado cuando la ley así lo permita; bien autorizando ella misma tratamientos por exigirlo el interés público, bien estableciendo que ante determinados datos, como los procedentes de fuentes accesibles al público, y en determinadas condiciones, no es necesario recabarlo"[255]. En el mismo sentido, el derecho a la protección de los datos se "sostiene sobre dos pilares fundamentales: el consentimiento y el conjunto de derechos que lo hacen practicable"[256].

En relación con lo dispuesto en el art. 6.2 LOPD, relativo a la no exigencia del consentimiento cuando los datos personales figuren en fuentes accesibles al público, el RGPD sólo establece que se debe informar a los interesados (en el caso de que los datos

profesional) facilita al profesional de la medicina información sobre su salud relativa a una afección genética que comparte con varios parientes cercanos. Asimismo, la paciente facilita al profesional médico determinados datos personales de los parientes (interesados) que también padecen la enfermedad. El profesional médico no está obligado a facilitar a estos parientes la información a que se refiere el artículo 14, ya que se aplica la excepción recogida en el artículo 14, apartado 5, letra d). Si el profesional médico lo hiciese estaría violando la obligación de secreto profesional que le debe a su paciente".

[255] MURILLO DE LA CUEVA, L., P., "El derecho a la autodeterminación informativa y la protección de datos personales", *Sociedad de Estudios Vascos*, San Sebastián, 2008, pp.43-58.

[256] SERRANO PÉREZ, M.M, *El derecho fundamental a la protección de datos. Derecho español y Comparado*, Aranzadi, Pamplona 2004, pp. 258-260.

no se hayan obtenido de estos), si los datos provienen de una fuente accesible al público. Sin embargo, estas fuentes, que en la LOPD estaban perfectamente definidas, en la normativa vigente no lo están, ya que sólo existe una mención muy escueta. Por ello, ante esta indefinición por parte de la LOPDGDD, considera que puede seguir aplicándose como criterio interpretativo la anterior LOPD; pero, no obstante, con la consideración de que debemos estar ante webs (abiertas) y fuentes en las que cualquier persona puede consultarlas, por lo que se excluyen aquellas que reducen su uso a usuarios limitados (redes sociales, por ejemplo).

El consentimiento se considera como la piedra angular de la privacidad y de la protección de datos, debido en gran parte a que permite garantizar la transparencia en el tratamiento de datos personales. Supone una manifestación de voluntad relacionada con el concepto de autodeterminación informativa, sobre la cual "la autonomía del titular de los datos es a la vez una condición previa al tratamiento y una condición para dotar de licitud el tratamiento de datos de carácter personal"[257].

El RGPD establece claramente que el consentimiento configura un presupuesto de licitud en materia de tratamiento de datos personales. Al mismo tiempo, determina que se entiende por consentimiento del afectado como *"(…) toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"*[258].

Podemos señalar, con ADSUARA VARELA, como la no validez del consentimiento tácito y la necesidad de recabar de nuevo el consentimiento, si se trata de tratamientos tácitos o expresos no adaptados a las exigencias del RGPD, como algunas de los aspectos del consentimiento que sufren variación respecto de la regulación del RGPD respecto de la LOPD y su Reglamento[259].

[257] MARTÍNEZ ROJAS, A., "Principales aspectos del consentimiento en el Reglamento General de Protección de Datos de la Unión Europea", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº42, 2016, pp. 4 y ss.

[258] Art. 6.1 LOPDGDD en relación con el art. 4.11 del RGPD.

[259] ADSUARA VARELA, Borja, "El consentimiento", en *Reglamento General de Protección de Datos …*, p. 168

Jurisprudencialmente, se pronuncia el TC, sobre la necesidad esencial de recabar el consentimiento del titular de los datos, señalando:

> *"(...)y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos". Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele (...)"*[260].

En el ámbito sanitario, destacar como la LBAP, dentro de los denominados "principios básicos", en el artículo 2, se refiere al respeto y dignidad de la persona humana y su autonomía, que se materializa a través de la exigencia previa del consentimiento del paciente, una vez informado adecuadamente, y su respeto, a través del derecho a la negación del tratamiento. Así, la regulación del consentimiento informado[261], prevista en los arts.8 a 10, íntimamente relacionada con el derecho a la autonomía del paciente (título del capítulo IV) supuso una gran novedad basada en el principio de autodeterminación o autonomía del paciente, superando ampliamente el concepto clásico de consentimiento informado que recogía la LGS.

[260] STC 292/2000, FJ 7.

[261] En el que el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del mismo (Considerando 42 del RGPD).

Situándonos en el contexto de la realización del acto médico-sanitario, la emisión de la información al paciente necesariamente habrá de prestarse como requisito ineludible para la posterior emisión del consentimiento del paciente del acto sanitario, el cual se realizará una vez recibida la información adecuada por el profesional sanitario, valorando las distintas opciones existentes. De esta forma, para poder tomar esta decisión o consentimiento por el paciente es requisito previo que haya sido informado a cerca de la naturaleza y finalidad de la intervención, así como sobre sus riesgos y consecuencias. Y este consentimiento informado, constituye un derecho fundamental, derivación del derecho a la vida, a la integridad corporal y a la libertad personal[262].

Estamos así, ante el "consentimiento informado[263]; de forma que su omisión o prestación defectuosa del mismo puede constituir infracción legal; por cuanto se parte del derecho de autodeterminación del paciente de poder decidir libremente sobre aquellas actuaciones que pueden afectar a su integridad corporal. No obstante, "no estamos ante un consentimiento informado, sino ante un deber de información y un posterior consentimiento; a una posterior decisión consciente y libre por parte del paciente debidamente informado"[264].

Así, esta información y el consentimiento informado de la que es manifestación, se constituyen en elemento esencial de la "*lex artis ad hoc*". Su omisión, cuando se materializan los riesgos típicos de los que el paciente no ha sido informado, puede generar responsabilidad. De hecho, supone una de las causas principales de condena de la responsabilidad civil médica.

2.1.4. PRINCIPIOS CONTENIDOS EN EL RGPD Y LA LOPDGDD

A diferencia de los principios de calidad, transparencia y consentimiento, examinados anteriormente y derivados de la normativa anterior, la regulación prevista en el RGPD y

[262] STC 37/2011, de 28 de marzo.

[263] "La conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud" (art. 3).

[264] LIZARRAGA BONELL, E., "La información y la obtención del consentimiento". La nueva Ley 41/2002, Básica Reguladora de la Autonomía del paciente", en *Autonomía del Paciente e información clínica*, Thomson-Civitas, Madrid, 2004, pp. 226-228.

en la LOPDGDD se muestra continuista respecto de sus normas predecesoras[265]: la Directiva 95/46/CE y la LOPD; cuyos artículos 4 a 12 contienen los siguientes principios:

2.1.4.1. Principio de licitud, lealtad y transparencia: tratados de manera lícita, leal y transparente respecto del interesado.

Licitud. El tratamiento de datos deberá ser lícito, para lo que deberá cumplir al menos una de las condiciones establecidas en el art. 6 RGPD, como veremos oportunamente al tratar el apartado de la legitimación del tratamiento. Se vincula este principio con el de transparencia, y éste a su vez con el de información, habida cuenta de que ésta debe prestarse de forma comprensible y accesible.

Transparencia. Resulta fundamental la aplicación del principio de transparencia al tratamiento de datos; referido a la información que deben recibir los interesados sobre la identidad del responsable del tratamiento y sus fines, así como la información necesaria para garantizar que sea leal y transparente respecto a los afectados y a su derecho a obtener confirmación y comunicación de los datos que les afectan y que son tratados[266].

Este principio está ligado al de información, como veíamos, y con la necesidad de que el tratamiento sea leal y lícito, y afecte a la información y su comunicación al interesado, que debe realizarse de forma sencilla; permitiendo ser accesible y entendible y comprensible con los fines del tratamiento; de forma que incluya "(…) *la identidad del responsable del tratamiento y sus fines, así como la información necesaria para garantizar que sea leal y transparente y a su derecho a obtener confirmación o comunicación de los datos que les afectan y que son tratados (…)*[267]; excluyendo, por tanto, cualquier tratamiento secreto o encubierto de los datos al margen de los supuestos legales.

Referido al ámbito de la salud, cobra, si cabe, más importancia de que el paciente reciba una información transparente sobre el tratamiento de sus datos de salud, en la medida en

[265] PIÑAR MAÑAS, J.L., "Jornadas ENATI sobre el Nuevo Reglamento Comunitario sobre Protección de Datos", CGAE, Madrid, 29 de abril de 2016.
[266] Considerando 39 RGPD.
[267] "Toda información y comunicación relativa al tratamiento de dichos datos será fácilmente accesible y fácil de entender, utilizándose un lenguaje sencillo y claro". Considerando 39 RGPD.

que pueda controlar que se realiza una utilización adecuada de los mismos. Particular trascendencia tiene la utilización (cesión de datos de salud) entre Administraciones públicas o dentro de la Administración sanitaria competente, destinada al ejercicio de sus funciones previstas legalmente, en las que no se comunica esta cesión al paciente afectado, que desconoce totalmente estos tratamientos por una Administración o Centro hospitalario distinto del que es el responsable del tratamiento de sus datos clínicos (médico del centro sanitario); de ahí que en estos casos debería realizarse, al menos, algún tipo de información al paciente.

Lealtad. Además, el tratamiento debe ser leal, de forma que para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

Se considera que se es leal en el tratamiento cuando se conoce la existencia de dichos tratamientos y, cuando los datos se obtengan de ellos mismos, contando con una información precisa y completa respecto a las circunstancias de dicha obtención[268]. De forma que no existiría lealtad si los datos se recaban sin que su titular conozca o se le informe sobre el tratamiento de sus datos.

Valga, para el caso de tratarse de datos de salud, lo señalado anteriormente respecto de la utilización o tratamiento de estos datos por las Administraciones públicas.

2.1.4.2. Principio de limitación de finalidad.

Los datos serán recogidos con fines determinados, explícitos y legítimos. Los cuales deben determinarse en el momento de su recogida, y no serán tratados ulteriormente de manera incompatible con dichos fines La recopilación de los datos debe darse bajo objetivos específicos, y no podrán usarse para ningún fin distinto para el que fueron recabados. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica.

[268] Considerando 38 Directiva 95/46/CE.

El Reglamento exige que para recoger los datos se deberán establecer previamente los fines para los que se obtienen, y deberá documentarse el uso futuro de los datos. Cuando un dato recabado con cierta finalidad quiere usarse para otra distinta, es necesaria la justificación por separado y autorización expresa de su titular; aunque las modificaciones posteriores de los objetivos inicialmente previstos están limitadas a determinadas circunstancias y bajo una justificación fundada. No obstante, podrán realizarse tratamientos de datos con finalidades distintas en la medida que se consideren las cuestiones previstas en el art. 6.4[269].

Tratándose de datos de salud, el objetivo primordial es la prestación de la asistencia sanitaria al paciente; aunque existen -como hemos visto- otras finalidades u objetivos distintos que suponen excepciones al afectar al conjunto de la población y que primarían sobre la protección individual, como puedan ser la salvaguarda de la protección del Estado, la salud pública de la población, la defensa o la seguridad pública.

Si manejamos datos de salud de personas trabajadoras con fines de archivos en interés público, fines de investigación científica e histórica o fines estadísticos, como es el tratamiento que compete realizar al Instituto Nacional de Seguridad y Salud en el Trabajo[270], a los órganos equivalentes en las CC.AA. o a la Administraciones Públicas Sanitarias[271], no se considera incompatible con el fin para el que han sido recogidos.

2.1.4.3. Principio de minimización de datos

Este principio se corresponde con la exigencia del "principio de adecuación de los datos, denomina por el Reglamento, en función de uno de sus matices, como principio de

[269] Art. 6.4 RGPD:
"(…) a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento; c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10; d) las posibles consecuencias para los interesados del tratamiento ulterior previsto; e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización".
[270] Art. 8 Ley 31/1995, de 8 de noviembre de Prevención de riesgos laborales.
[271] Art. 10 Ley 31/1995, de 8 de noviembre de Prevención de riesgos laborales.

minimización de datos[272]. Así, los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, lo que requiere que se limite de forma estricta un plazo mínimo de conservación. Por tanto, en el ámbito sanitario, sólo deberán utilizarse los datos mínimos indispensables necesarios para que pueda atenderse al estado de salud del paciente, incorporándose a la HC del paciente aquellos que son absolutamente imprescindibles para el proceso curativo. Este principio se correspondería con el principio de proporcionalidad de la anterior LOPD y que el nuevo Reglamento modifica en cuanto que los datos personales ya no deberán ser "excesivos" según la finalidad para la que se recabaron, sino "necesarios".

De esta forma se refuerza el sentido de "necesarios", para señalar que, si el objetivo perseguido puede conseguirse sin llevar a cabo el tratamiento de datos, éstos no deben ser tratados; por lo que debe llevarse a cabo una evaluación previa de la cantidad y categoría de los datos a utilizar, ya que "Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios"[273].

2.1.4.4. Principio de exactitud y veracidad

Los datos serán exactos, y si es posible actualizados, suprimiéndose los que sean inexactos respecto de los fines para los que son tratados.

Tratándose de datos de salud, ya vimos la importancia de que el profesional médico realice sus funciones con datos veraces, exactos y, sobre todo actualizados, debido a la importancia de que la tarea curativa se aplique sobre los últimos datos diagnósticos del paciente. Además, puede considerarse una medida necesaria a aplicar en determinadas instancias el mantener un registro de los datos incorrectos, cuando se trataran datos de salud de un paciente.

[272] PUYOL MONTERO, J., "Los principios del derecho a la protección de datos", en *Reglamento General de Protección de datos…,* p. 138.
[273] Considerando 39 RGPD.

2.1.4.5. Principio de limitación del plazo de conservación

Los datos serán mantenidos identificando a su titular durante el tiempo indispensable para los fines del tratamiento. De forma que los datos habrán de mantenerse sólo durante el tiempo necesario requerido por los fines del tratamiento. Excepcionalmente podrá prolongarse el tiempo de conservación cuando se trata de datos con fines de archivo, interés público, investigación científica o histórica y fines estadísticos. Corresponde al responsable del tratamiento incluir plazos de supresión o revisión periódica[274].

En el ámbito sanitario, como hemos visto al hablar de la HC, debe conservarse por un plazo mínimo de cinco años (o más según normativas de las CCAA) o el que resulte necesario en función del tipo de patología que afecte al paciente. En todo caso, habrá de tenerse en cuenta que estamos ante un plazo legal mínimo, pero que en todo caso debe estar supeditado a la propia evolución y estado médicos del paciente, cuyo tratamiento médico pueda necesitar de la comprobación de datos de tiempo superior al mínimo, como pueda suceder con los pacientes en tratamiento crónico y permanente. Además, este principio debe contemplar la hipotética necesidad de que el paciente necesite la HC como prueba en una reclamación o proceso de negligencia sanitaria o de reclamación de una indemnización sanitaria[275].

Además, referido a la HC:

"*La historia clínica deberá conservarse en las condiciones que garanticen la autenticidad, integridad, confidencialidad, preservación y correcto mantenimiento de la información asistencial registrada, y que asegure una completa posibilidad de reproducción en el futuro, todo ello durante el tiempo en que sea obligatorio conservarla e independientemente del soporte en que se encuentre, que podrá no ser el original*"[276].

La AEPD señala, con base en el art. 17 LBAP, que los centros sanitarios tienen la obligación de conservar la historia clínica en los términos y plazos señalados en dicho

[274] Considerando 39 RGPD.

[275] ATELA BILBAO, A., y otros, *Autonomía del paciente, información e Historia clínica. Estudios sobre la Ley 41/2002, de 14 de noviembre*, GONZÁLEZ SALINAS y LIZARRAGA BONELLI (coords), Edit, Thomson-Civitas, Pamplona, 2004, p. 65.

[276] Art. 9 Decreto 38/2012, del País Vasco, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.

precepto; lo que lleva a que en la práctica realmente el ejercicio de estos derechos quede limitado a los datos erróneos o desproporcionados[277].

En el caso de investigación biomédica, puede procederse a la seudonimización de los datos, separando los datos identificativos de la personalidad del paciente de lo que son datos de salud; sin que ello impida volver a asociarlos si fuera necesario.

2.1.4.6. Principio de integridad y seguridad.

Los datos serán tratados de forma que se garantice su seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito, su pérdida y destrucción o daño accidental, a través de medidas técnicas u organizativas apropiadas.

De acuerdo con este principio, los que traten tus datos personales deben actuar proactivamente con el objetivo de protegerlos frente a cualquier riesgo que amenace su seguridad.

Otro de los principios destinados a ofrecer garantías entorno al tratamiento de datos, es el referido a los datos especialmente protegidos que busca un reforzamiento de protección sobre los derechos y libertades de los interesados"[278].

Respecto a la seguridad de los datos de salud, nos remitimos a lo indicado en el apartado específico de "Seguridad de los datos sanitarios" (Título I.4).

2.2. DERECHOS DE LOS TITULARES DE DATOS

2.2.1. OTRA CLASIFICACIÓN, DISTINTA DE LOS DERECHOS ARCO

A pesar de la falta de vigencia de la LOPD y su Reglamento, siguen resultando muy útiles sus postulados[279], mantenidos o matizados en muchas ocasiones por la nueva regulación

[277] Entre otras Resolución AEPD, R/00549/2004, de 6 de octubre de 2004.
[278] AEPD, Guía sobre protección de datos.
https://www.aepd.es/media/guias/guia-ciudadano.pdf
[279] LOPDGDD. Disposición adicional decimocuarta. *Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE. "*Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del

de la materia, necesitándose su invocación ante problemas interpretativos o de vacío legal existentes. Así, los datos de carácter personal pueden estar presentados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, que únicamente podían pertenecer a personas físicas identificadas o identificables[280]; sin que la normativa sea de aplicación a los datos referidos a personas jurídicas ni a personas fallecidas, como la AEPD había ratificado en sus informes[281], y que la propia LOPDGDD se ha encargado de matizar, sobre la base del postulado de la LOPD, al otorgar a familiares, herederos o personas vinculadas (parejas de hecho) al fallecido, el derecho de acceso, rectificación e incluso supresión de los datos digitales, salvo prohibición expresa de una ley o del finado antes del fallecimiento (art. 3).

Los derechos ARCO están íntimamente relacionados con el derecho de información previa. Así, el derecho de protección de datos no solamente implica la existencia de instrumentos legales que permiten al titular de los datos gozar de una autentica disposición de su información personal, con la exigencia de manifestar su consentimiento previo al uso de sus datos personales; también conlleva el hecho de ser informado previamente, de modo expreso, preciso e inequívoco sobre el destino que le darán a los mismos, acceder a los contenidos que los incluyan, rectificación y hasta eliminación a solicitud del interesado.

Las facultades reconocidas al titular del derecho a la protección de datos personales, agrupadas en un subconjunto de derechos llamado ARCO[282], configurados en base a la anterior normativa de protección de datos, se han visto ampliados y modificados por el RGPD[283] y la LOPDGDD, con el reconocimiento del derecho al Olvido (derecho de supresión), el derecho a la portabilidad, limitación del tratamiento y a no ser objeto de decisiones individualizadas; pudiéndose ejercer directamente o mediante representante,

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, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas".

[280] Artículo 3.a).

[281] Es oportuno recordar que el artículo 13 de la Ley 12/1989, de 9 de mayo, de la función pública estadística, emplea una noción de dato personal referida tanto a personas físicas como jurídicas.

[282] En opinión de DAVARA RODRIGUEZ, tienden a desaparecer. DAVARA RODRÍGUEZ, M., "Una primera aproximación al Reglamento europeo de protección de Datos y su incidencia en el tratamiento de datos de carácter personal de las Administraciones Públicas", *Actualidad Administrativa*, N° 4.

[283] Arts. 15 a 22 RGPD y 18 a 22 LOPDGDD.

mediante solicitud dirigida al responsable del tratamiento. De esta forma, la protección del titular o persona física identificada o identificable a la que se refieren sus datos personales, como titular del derecho a la protección de datos de carácter personal, se instrumenta a través de los denominados derechos ARCO (ampliados), que tienen un carácter gratuito y personalísimo; al mismo tiempo que su falta de atención o inobservancia faculta a los afectados a interponer un proceso de tutela de derechos ante la autoridad de protección de datos[284].

El titular de los datos personales detenta el derecho de acceso, o *habeas data*, para solicitar y obtener gratuitamente información de sus propios datos de carácter personal sometidos a tratamiento, la fuente de esos datos, así como las comunicaciones realizadas o por realizarse[285]. El derecho de acceso, por tanto, es la herramienta que impulsa al Derecho a la protección de datos personales y requiere, como condición previa para su tutela, la posibilidad de conocer qué datos ligados a una determinada persona están en poder del responsable o encargado del tratamiento y la finalidad que se persigue[286].

El principio de la autodeterminación informativa, materializado a través del poder de disposición y control de sus propios datos personales por parte de su titular [287], como hemos visto, consiste en la facultad que posee el titular de un dato de carácter personal a conocer, acceder, rectificar, cancelar y controlar la información que le sea inherente; de forma que estos derechos de acceso, rectificación, cancelación u oposición al tratamiento,

> *"(…) constituyen un haz de facultades que emanan del derecho fundamental a*

[284] Para más información sobre los derechos ARCO véase la Guía para el ciudadano de la AEPD:https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO.pdf

[285] De acuerdo con la SAN de 19 de marzo de 2014 "(…) el derecho de acceso sólo alcanza a los datos personales del titular (…) sin que quepa aceptar que incluye el derecho a acceder a datos de carácter personal de otras personas, pues ello comportaría la vulneración de su derecho fundamental a la protección de datos, consagrado en el art. 18.4 CE"

[286] STEINMEYER ESPINOSA, A., "¿Permite el derecho de acceso a la información pública, el acceso a datos personales?, Universidad Tecnológica Metropolitana. *Serie Bibliotecología y Gestión de Información* N° 79, Chile, 2013, p. 10.

[287] Para MURILLO DE LA CUEVA consiste en "el control que a cada uno de nosotros corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia identidad, nuestra dignidad y libertad. En su formulación como derecho, implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos, que desea que no se conozcan, así como facultades que le aseguren que los datos que de su persona manejan terceros informáticamente son exactos, completos y actuales, y que se han obtenido de modo leal y lícito". MURILLO DE LA CUEVA, P.L., *Informática y protección de datos personales (estudios sobre la Ley Orgánica 5/1992, de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal), op.cit.*, p. 32.

> *la protección de datos y sirven a la «capital función que desempeña este derecho: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer(...). Este derecho faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero o cuáles puede un tercero recabar, y, también, le permite saber quién posee esos datos personales y para qué, pudiendo oponerse a su posesión o uso». El titular del dato para hacer efectivo tal contenido puede «exigir del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos y qué destino han tenido, y, en su caso, requerirle para que los rectifique o los cancele"*[288].

Era posible denegar los derechos de acceso, rectificación y cancelación de los datos, de acuerdo al apartado 2 del art. 24 de la LOPD, si " (…) *ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante (...) intereses de terceros más dignos de protección*". Ello, suponía la fijación de un límite genérico al derecho fundamental a la protección de los datos de carácter personal, ya que no se establecía cuáles podrían ser esos intereses ni las circunstancias en las que se podían hacer valer para restringir de esa forma este derecho fundamental.

De esta forma, una denegación de acceso, rectificación o cancelación de datos personales podría considerarse arbitraria, al margen de que esos intereses puedan identificarse con los derechos fundamentales de ese tercero o con cualquier otro interés que pudiere esgrimirse, dada la inconstitucionalidad de este y otros preceptos, por los cuales se establecían cautelas para restringir los derechos de acceso y cancelación de los datos obrantes en las AAPP[289].

Este planteamiento, en cuanto al límite al derecho de acceso a la información pública que suponía la LOPD, se ha visto clarificado y delimitado a través de la introducción de los

[288] STC 292/2000, FJ 7.

[289] SAN de 31 de marzo de 2015. Desestima el recurso contencioso-administrativo interpuesto contra una Resolución del Director de la AEPD, de 19-09-2013, sobre derecho de acceso a datos personales.

límites y criterios específicos establecidos en los arts. 14 y 15 de la LTBG[290], y que será objeto de tratamiento específico en el apartado III.2.

Por su parte, el RGPD ha venido a suponer un reforzamiento en el control que las personas tienen sobre sus datos personales, lo que se traduce en un mayor catálogo de derechos de los interesados, que incluye algunos derechos novedosos, recogidos en la Directiva 95/46/CE[291]; por lo que ahora ya no debe hablarse de derechos ARCO, sino de nuevos derechos.

Como todos los derechos, los derechos ARCO y, más en concreto los derechos previstos en los arts. 12 a 22 del RGPD, no tienen un contenido absoluto, por lo que son susceptibles de limitaciones, al igual que los derechos actualizados o novedosos derivados del RGPD y la LOPDGDD. La Directiva 95/46/CE, recogía detalladamente las excepciones y limitaciones de estos derechos por parte de los Estados miembros, en la medida que estas limitaciones constituyeran una medida necesaria para salvaguardar la seguridad del Estado, prevención y represión de delitos, etc.

En este sentido, el RGPD contempla la posibilidad de limitar, por parte del Derecho de la Unión o de los Estados miembros, mediante medidas legislativas, los derechos y obligaciones contenidos en los arts. 15 a 22 y arts. 5 y 34, con la condición de que "(…) *esta limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar*": la seguridad del Estado, la defensa y seguridad pública, etc. (art. 23).

Respecto de los datos especialmente protegidos, el Reglamento establece que "*Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud*"[292]; lo que va a permitir que, por ejemplo, el Estado español pueda dictar legislación específica de ámbito sanitario o de salud en la que se contengan condiciones específicas propias de este ámbito e incluso limitaciones en el tratamiento de estos datos, como la LBAP o la Ley de Salud Pública.

[290] Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
[291] ÁLVAREZ CARO, M., "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones…", en *Reglamento General de Protección de Datos…*, *op.cit.*, pp. 228 y ss.
[292] Art. 9.4 RGPD.

Los derechos reconocidos en los arts. 15 a 22 RGPD están íntimamente relacionados con los propios principios del derecho de protección de datos, los cuales deberán ser exactos, completos y actualizados, y con la propia autodeterminación informativa vinculada al poder de control por la persona de sus propios datos. Podrán ejercerse directamente o mediante representante legal o voluntario (art. 12 LOPDGG).

A continuación, pasamos a analizar los distintos derechos de que disponen los titulares de datos personales.

2.2.1.1. Derecho de rectificación

Podemos encontrar una primera definición en la CDFUE como "(…) *el derecho que tiene el interesado cuando los datos personales son inexactos o están incompletos, a instar al responsable del tratamiento que rectifique esos datos*". Con ello, se intenta garantizar que sea exactos, y tratados lícitamente. Por su parte, el RGPD indica que "(…) *todo interesado debe tener derecho a que se rectifiquen los datos personales que le conciernen*" (Considerando 65).

El interesado tendrá derecho a solicitar la rectificación de los datos inexactos que le afecten, además de que los datos que sean incompletos sean completados, considerando los fines del tratamiento; acompañando a dicho fin la documentación que demuestre dicha inexactitud o falta de plenitud[293]. Además, supone uno de los motivos que condicionan la licitud del tratamiento: el que el responsable del tratamiento adopte las medidas adecuadas para rectificar los datos personales inexactos de inmediato.

Los datos personales serán rectificados o suprimidos cuando el tratamiento no cumpla lo regulado en la LOPDGDD, o que esos datos resulten inexactos o incompletos, aunque a juicio de algunos autores, la rectificación (artículo 14) y la supresión (artículo 15) se diferencian además, por su aplicación: la rectificación procederá cuando los datos sean erróneos o inexactos; en cambio la supresión se aplica cuando sean inadecuados o excesivos respecto a la finalidad del tratamiento, pero también es posible suprimir la información cuando el consentimiento haya sido revocado.

[293] Arts. 16 RGPD y 14 LOPDGDD.

Al rectificar no se busca borrar o destruir físicamente la información sino la "(…) *sustitución de datos personales inexactos o incorrectos por otros actuales y correctos, pero siempre que no exista desviación del fin, o un uso desproporcionado de los mismos*"[294].

La LORTAD preveía evitar que la cancelación (ahora supresión) pudiese causar un perjuicio a los intereses legítimos del afectado, de terceros, o simplemente cuando no se cumpliera la obligación de conservar los datos. Sin embargo, en la LOPDGDD no se contempla esa excepción expresamente, pero sigue vigente la conservación de los datos cuando así lo dispongan las normas o cláusulas contractuales que regulan las relaciones entre los responsables del tratamiento y los interesados.

La LOPD y su Reglamento, se referían al derecho de cancelación, el cual dará lugar a la supresión de los datos que resultaran inadecuados o excesivos, sin perjuicio del deber de bloqueo de los mismos. De forma que, mediante el bloqueo se identifican y reservan los datos con el objeto de impedir su tratamiento. No obstante, los datos que se bloquean después de la supresión estarán disponibles para las administraciones públicas, jueces y tribunales. También podrán utilizarse para atender cualquier responsabilidad producto del tratamiento en los plazos previstos, y una vez prescritos los intervalos temporales se suprime la información[295]. De esta forma, el bloqueo viene a suponer un efecto derivado de la propia cancelación de los datos.

Según la AEPD, el bloqueo debe efectuarse "de forma que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso; por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia"[296].

Señalar, que estamos ante un derecho independiente, de ejercicio autónomo, y personalísimo. Corresponde al responsable del tratamiento identificar al interesado que

[294] Arts. 16 RGPD y 14 LOPDGDD.
[295] Arts. 16.3. LOPD y 5.1.b) RLOPD.
[296] AEPD, Informe de 5 de junio de 2007.

desea ejercer su derecho de rectificación a través de medios adecuados, solicitándole la información necesaria para verificar la exactitud de los datos y la personalidad del interesado. Además, tanto el interesado como el responsable del tratamiento habrán de prever si los datos son, en la medida adecuada, los necesarios para el cumplimiento de la finalidad prevista; ya que, siendo insuficientes, pueden ser completados por el propio interesado, accediendo directamente a sus propios datos y rectificándolos; o bien, a través de una declaración adicional que dirigirá al responsable para que éste complete los datos que tiene en su poder, considerándose, en este caso, que con esta rectificación existe un tratamiento de datos.

Tratándose del ámbito sanitario, el paciente interesado tiene derecho a que se rectifiquen en su HC sus datos personales inexactos por parte del responsable del tratamiento y a completar aquellos datos que sean incompletos. La rectificación se realizará aportando la documentación que acredite la carencia o error de los datos, correspondiendo al profesional sanitario determinar si procede o no la rectificación[297].

2.2.1.2. Derecho de cancelación

Frente al derecho de rectificación, contemplado en el art. 16 del RGPD, coincidente con el derecho de cancelación de la normativa anterior sobre protección de datos, el RGPD se refiere al derecho de supresión (derecho al olvido), en su art. 17, para, en un sentido más amplio que el clásico de la cancelación, incluir la supresión de los datos en las distintas circunstancias previstas en dicho artículo, y que se analizarán detalladamente en el apartado del derecho de supresión o derecho al olvido.

La AEPD se ha pronunciado frecuentemente sobre la cancelación de datos sanitarios contenidos en la HC. Considera que, de acuerdo con lo dispuesto en el artículo 15.2 LBAP, en la historia clínica deben constar los datos que permitan el conocimiento veraz y actualizado del estado de salud del paciente. La determinación de qué datos permiten alcanzar dicha finalidad corresponde al médico[298].

[297] AEPD, Guía para pacientes y usuarios de la Sanidad, noviembre 2019.
[298] Entre otras Resolución de la Agencia Española de Protección de Datos R/00549/2004, de 6 de octubre de 2004.

2.2.1.3. Derecho de limitación del tratamiento[299].

Se define por el propio RGPD, señalando que, se refiere a "(…) *el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*" (artículo 4.). Se trata, por tanto, de una medida cautelar que permite la suspensión del tratamiento de datos en supuestos de impugnación por el titular de la exactitud de los datos, para el ejercicio de reclamaciones, en el caso de oponerse a la supresión de los datos personales tratados ilícitamente, o se haya opuesto a un tratamiento legítimo por afectar a su situación particular. Corresponde al responsable del tratamiento comunicar la puesta en marcha y el cese de la medida adoptada.

Por ello, el interesado tendrá derecho a la limitación del tratamiento de sus datos, de forma que sólo se llevará a cabo el tratamiento con su consentimiento, o sea necesario para formular reclamaciones, protección de derechos de terceros, o razones de interés público. Deberá constar esta limitación en los sistemas de información del responsable. Procederá esta limitación, salvo en los siguientes supuestos:

a) Cuando se impugne su exactitud durante un plazo que permita su verificación por el responsable;

b) Si existe un tratamiento ilícito y el interesado se oponga a su supresión, solicitando en su lugar la limitación de uso;

c) Aunque el responsable no necesite los datos para los fines del tratamiento el interesado si le sean útiles para formular reclamaciones;

d) El interesado se haya opuesto al tratamiento en virtud del artículo 21.1., mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

En cuanto a los métodos para limitar el tratamiento de datos, "(…) *cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento*

[299] Arts. 18 RGPD y 16 LOPDGDD.

ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema[300].

Trasladándonos al ámbito sanitario, la aplicación de este derecho resulta excepcional, por cuanto la prioritaria prestación de la asistencia sanitaria al paciente no permite que pueda limitarse el tratamiento de datos de salud.

Con ocasión de la actual epidemia de coronavirus, la AEPD ha emitido un informe sobre el tratamiento de los datos de salud durante la pandemia, señalando su licitud si se realiza conforme al RGPD; al mismo tiempo que recuerda que el tratamiento de este tipo de datos debe respetar los principios recogidos en el RGPD, como el de limitación del tratamiento, señalando, indicando, asimismo, que otras agencias de protección de datos, como las de Reino Unido y Francia, se han pronunciado en relación a esta situación, señalando la necesidad de que se limite al máximo el tipo de datos que se recaban y sus finalidades, concluyendo con la recomendación de no recabar datos de salud si existen otros medios alternativos menos invasivos para la misma finalidad (por ejemplo, en lugar de preguntar a los trabajadores por determinados síntomas de salud, se les informe de que si tienen esos síntomas o han estado en zonas de riesgo o se han relacionado con personas con síntomas, acudan al servicio médico).

Las agencias de protección de datos de Reino Unido y de Francia, entre otros países, se han pronunciado también al respecto de esta situación, siendo elemento común a ambas la necesidad de limitar al máximo el tipo de datos que se recaban y las finalidades, recomendando que, en la medida de lo posible, no se recaben datos personales de salud si existen otros medios menos invasivos para la misma finalidad (por ejemplo, que en lugar de preguntar síntomas a los trabajadores, se informe a estos de que si han estado en zonas de riesgo o presentan síntomas deben acudir a un servicio médico)[301].

[300] Considerando 67 RGPD.
[301] AEPD, Informe sobre tratamiento de datos en relación con el COVID-19, 12 de marzo de 2020.

2.2.1.4. Derecho de oposición[302] y decisiones individuales automatizadas

Además de los derechos relacionados con las decisiones individuales automatizadas, que veremos seguidamente, incluida la realización de perfiles[303], el interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que los datos personales que le conciernan sean objeto de un tratamiento basado en que el mismo es necesario: a) para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; b) para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero (no se aplica si estamos ante tratamiento realizado por autoridades públicas en el ejercicio de sus funciones[304]), incluida la elaboración de perfiles sobre la base de dichas disposiciones.

El interesado podrá oponerse al tratamiento (derecho a la limitación del tratamiento) de sus datos utilizados con fines de mercadotecnia directa en todo momento, incluida la elaboración de perfiles relacionados con la mercadotecnia[305], dejando de ser tratados para estos fines. Del mismo modo, en el ámbito de la sociedad de la información, podrá oponerse por medios automatizados que apliquen especificaciones técnicas.

En el ámbito sanitario, considerando la finalidad curativa de la asistencia sanitaria prestada por profesionales sanitarios y la utilización de datos personales de salud en beneficio del paciente, debe entenderse que la aceptación de este derecho debe tener carácter excepcional, en la medida en que no puede impedir o dificultar la práctica asistencial. Así, uno de los supuestos (excepcionales) en los que podría darse sería en el supuesto de las Instrucciones Previas o Voluntades anticipadas, en las que con carácter anticipado la persona dispone que para un futuro no se lleven a cabo una serie de actuaciones médicas sobre su cuerpo (básicamente de evitación de medidas infructuosas), lo que, indudablemente lleva aparejado que no se utilicen los datos clínicos del paciente, quedando "congelados", por su propia decisión; salvo que, a criterio médico, no deban realizarse las indicadas medidas proscritas anticipadamente por el paciente.

[302] Considerando 69 RGPD, Arts. 21 y 22 RGPD y 18 LOPDGDD.
[303] Cuya regulación se contiene en el art. 22 RGPD.
[304] Art. 6. 1.e) y f) RGPD.
[305] Considerando 70 RGPD.

Así mismo, el interesado tendrá derecho de oposición, en relación con datos personales tratados con fines de investigación científica o histórica o fines estadísticos, excepto que el tratamiento fuese necesario para el cumplimiento de una misión realizada por razones de interés público.

2.2.1.4.1. Decisiones individuales automatizas

En una primera aproximación al tema, encontramos que el RGPD, en su art. 63, contempla como, entre otros derechos, "(…) *todo interesado tiene derecho a conocer y a que se le comunique (...) la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles*[306], *las consecuencias de dicho tratamiento (...)".*

No estamos ante un derecho novedoso, por cuanto tenía existencia reconocida, tanto en el derecho europeo (art. 15 Directiva 95/46/CE), como en nuestro ámbito nacional (art.13 LOPD), y el GT29 se refería al mismo, en la medida de que estamos ante una prohibición incluida en el RGPD, por la que el responsable del tratamiento no puede adoptar una decisión basada únicamente en el tratamiento automatizado, que debe aplicarse al margen de que el interesado ejerza o no su derecho de oposición.

El propio Considerando 71 del RGPD alude a que "(…) *el interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar y, como ejemplo, apunta la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna(…)*".

Además, este tipo de tratamiento incluye la elaboración de perfiles, los cuales *"(...) consisten en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos*

[306] Conforme a la definición del art. RGPD se definen como "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física".

relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar".

Por tanto, en virtud de este derecho, el interesado afectado por el tratamiento de sus datos personales puede requerir al responsable del tratamiento a fin de no ser objeto ni estar afectado por una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre él o le afecte significativamente de modo similar[307].

Además, el precepto general de prohibición, configurado como derecho del interesado sobre decisiones individuales basadas únicamente en un tratamiento automatizado, de acuerdo con el apartado 2 del artículo 22 RGPD, no resulta aplicable cuando 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.

Sin embargo, las excepciones aplicativas anteriores quedarían inaplicables tratándose de decisiones individuales basadas en datos de salud y, por tanto, de datos especialmente protegidos, salvo que:

a) El interesado haya dado su consentimiento explícito;

b) El tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, Además, el responsable del

[307] En relación con la necesidad de que no haya intervención humana en el tratamiento al tratarse de un tratamiento automatizado, el GT29 entiende por intervención humana, que la persona que intervenga deba tener la autoridad y capacidad para poder cambiar o modificar una decisión: *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, adoptadas el 3 de octubre de 2017.

tratamiento haya tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

De ahí, que sectores especialmente sensibles, como el sanitario o de la salud, puedan justificar el que en determinados ámbitos de la misma puedan rechazarse este tipo de tratamiento mediante decisiones automatizadas[308].

2.2.1.5. Derecho a la supresión o al olvido

Pese a que novedosamente se incluye así en el RGPD, no estamos ante un derecho nuevo, sino ante la manifestación del derecho a la cancelación de datos en el entorno de Internet, unido estrechamente a la evolución del derecho a la intimidad y al derecho a la protección de datos personales. Así, "Supondría una concreción del derecho de oposición y cancelación en un caso concreto como es el tratamiento de datos en Internet"[309]. Es, por tanto, un producto de la sociedad de la información, antes de la cual "las fronteras de la privacidad estaban defendidas por el tiempo y el espacio"[310].

Este derecho tiene sus antecedentes doctrinarios en la Sentencia del 13 de mayo de 2014 del TJUE en autos "Google Spain SL c/Agencia Española de Protección de Datos", en la que se consolida el derecho al olvido, siendo, así, objeto de reconocimiento jurisprudencial en relación al tratamiento de los datos por motores de búsqueda de internet.

En dicha sentencia se reconoce el derecho del interesado de suprimir o bloquear información de los motores de búsqueda tanto en el caso de datos inexactos como en aquellos casos que, si bien son exactos, los mismos hayan sido obtenidos sin su

[308] MARTÍNEZ MARTÍNEZ, R: "Big data, investigación en salud y protección de datos personales. ¿un falso debate?", *Revista valenciana d'estudis autonòmics*, Nº 62, 2017, págs. 235-280, pág. 270.

[309] Como señala ÁLVAREZ CARO, M., "El derecho a la supresión o al olvido", en *Reglamento General de Protección de Datos…*, *op.cit*., pp. 241 y ss., refiriéndose además a la denominación empleada por LÓPEZ GARCÍA, M., "Derecho a la información y derecho al olvido en Internet", *La Ley Unión Europea*, nº 17, julio 2014, p. 49.

[310] PIÑAR MAÑAS, J.L., "Códigos de conducta y espacio digital. Especial referencia a la LOPD", en *Datos personalesorg. La Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 44, 2010.

consentimiento o su tratamiento no sea adecuados, su conservación sea excesiva, o se contradigan con las prescripciones legales en la materia.

Además, no solo se podrá ejercer el derecho en función de que los datos sean inexactos, sino en particular "*(...) de que sean inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, que no estén actualizados o de que se conserven durante un período superior al necesario, a menos que se imponga su conservación por fines históricos, estadísticos o científicos*"; agregando que a petición del interesado deberán eliminarse aquellos datos que hubieran sido recabados de forma lícita pero que devengan ilícitos cuando los mismos "(…) *ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Este es el caso, en particular, cuando son inadecuados, no pertinentes, o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido"*[311].

En el mencionado pronunciamiento, el TJUE, establece que la entidad que desarrolla y administra los motores de búsqueda es la responsable por el tratamiento que dichos motores realizan con los datos, y que dicho tratamiento se encuentra sujeto a las normas de protección de datos nacionales, siempre que dicha entidad realice sus actividades desde uno de los Estados miembros o cuando la actividad sea dirigida a ciudadanos de dichos Estados. Así mismo, se reconoce el derecho de las personas a solicitar que se supriman datos que los afecten aun cuando dicha información no haya sido eliminada por el editor de esta. Conforme a todo lo expresado, podemos afirmar que dicha sentencia ha sido una aportación fundamental y ha configurado lo que hoy se conoce como doctrina del olvido, que resolvió de forma favorable la pretensión del Estado español a través de la AEPD.

En definitiva, se establece que los motores de búsqueda de internet se encuentran obligados a hacer efectivo los derechos de oposición, supresión y cancelación a solicitud del interesado, sobre quien recae la carga de dirigirse al buscador para solicitarle el cese de la difusión de sus datos cuando la misma afecte algún derecho del interesado, siempre que dicho cese no interfiera con derechos de terceras personas a la referida información. Tal es el caso de las personas públicas, o cuando el conocimiento de dichos datos tuviera

[311] Sentencia del TJUE (Gran Sala), de 13 de mayo de 2014, asunto C-131/12 -EU:C:2014:317, Google Spain SL contra La Agencia Española de Protección de Datos.
Disponible en: http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

una relevancia pública, a fin de armonizar el presente derecho con el principio de transparencia y acceso a la información pública.[312].

Por este motivo, el derecho al olvido es considerado como un derecho no absoluto, quedando limitado por el resto de derechos fundamentales y por los bienes constitucionalmente protegidos en aplicación de la doctrina de los límites de los derechos fundamentales[313]; en el entendido que dicho derecho podrá ser ejercido siempre que el mismo no se oponga al ejercicio de otro derecho fundamental de un tercero o que su supresión no vulnere el interés público. En este sentido, la mencionada sentencia proporciona determinadas pautas para resolver un hipotético conflicto entre el derecho de cancelación y los derechos de interés públicos existentes, estableciendo que el derecho de cancelación,

> "(…) *prevalece, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en encontrar la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información que se trate"*.

Esta sentencia sentó precedente en la materia, resaltando la necesidad de regular de forma uniforme y vinculante entre los Estado europeos el derecho al olvido con la finalidad de proteger los intereses de los titulares de datos ante la llegada de las tecnologías de información, la universalización y alcance de los motores de búsqueda de internet, como modo de tutelar el derecho a la protección de datos en la UE.

De esta forma, la nueva doctrina del derecho al olvido ha supuesto una importante aportación, que orienta la innovación jurídica en materia de protección de datos; al considerar de forma específica que determinadas prácticas desarrolladas en entornos

[312] MURILLO DE LA CUEVA, L., "Las vicisitudes del derecho de la protección de datos personales*", Revista Vasca de Administración Pública,* Vol. Nº58, 2000, pp. 211 a 235.
[313] STC 17/2013, de 31 de enero.

digitales no sean conformes a Derecho[314]. No obstante, queda clara la preferencia de la protección de datos sobre los intereses económicos de los operadores del motor de búsqueda.[315]

Situándonos en el ámbito nacional, encontramos sentencias en el mismo sentido[316], en las que establece que el mencionado derecho al olvido puede ser desplazado por intereses de relevancia constitucional, siempre que dicha restricción se justifique en alcanzar el fin legitimo superior. Igualmente, la STC 545/2015, de 15 de octubre, por la que se confirmó la adopción de medidas tendentes a impedir que los motores de búsqueda de internet pudieran detectar la noticia a partir de la introducción del nombre y los apellidos de los afectados. Sin embargo, en cuanto a la eliminación del nombre y apellidos de la página web del «El País», consideró que la misma suponía una medida desproporcionada, porque invadía el campo de la libertad de información.

Esta sentencia, define el derecho al olvido de acuerdo con el planteamiento contenido en el art. 17 RGPD como "(…) *el derecho a obtener, sin dilación indebida, del responsable del tratamiento de los datos personales relativos a una persona, la supresión de esos datos, cuando ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados; cuando se retire el consentimiento en que se basó el tratamiento; cuando la persona interesada se oponga al tratamiento; cuando los datos se hayan tratado de forma ilícita; cuando se deba dar cumplimiento a una obligación legal establecida en el Derecho de la Unión Europea o de los Estados miembros; o cuando los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información"* (FJ 5).

De Esta forma, para el TC, el derecho al olvido como derecho de supresión de datos personales, forma parte del art. 18.4 CE, constituyendo un derecho fundamental al integrarse en las libertades informáticas contenidas en este artículo. En consecuencia, el derecho al olvido, además de ser un derecho autónomo, actúa también como mecanismo

[314] Como pone de manifiesto DOPAZO FRAGUIO, P., "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente", *Revista Española de Derecho Europeo* nº 68/2018, Civitas, Aranzadi, Pamplona, 2018, pp.113-148; refiriéndose a RALLO LOMBARTEI, A., "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018), *Revista de Derecho político*, nº 100, 2017, pp. 639-666.

[315] STJUE, de 13 de mayo de 2014.

[316] SSTC 57/1994, de 28 de febrero y 18/1999, de 22 de febrero.

de garantía para la preservación de los derechos al honor y a la intimidad, dada la relación existente entre los apartados 1 y 4 del artículo 18 CE; de manera tal que el 18.4 opera como garantía de los derechos del 18.1 , siendo "(…) *instituto de garantía como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, pero que es también, en sí mismo, un derecho fundamental(…)*"[317].

Por parte de la jurisprudencia no constitucional, el TS ha tenido ocasión de pronunciarse sobre el contenido de este derecho de la siguiente forma:

> *" El llamado "derecho al olvido digital", que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos (...). Pero dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse a un tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como el nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su persona, provocando un efecto estigmatizador*[318].

Así, en este contexto de necesidad de que el derecho del interesado a cancelar sus datos se acomode a la nueva generación electrónica y, en concreto, de la Red Internet de los

[317] STC 25471993, de 20 de julio (FJ 6) y STC 290/2000 (FJ 7).

[318] STS de 15 de octubre de 2015. El Tribunal Supremo estima parcialmente recurso de casación por "Ediciones El País, S.L.", contra la sentencia núm. 486/2013, dictada el 11 de octubre de 2013 por la Audiencia Provincial de Barcelona, en el recurso de apelación núm. 50/2013.

prestadores de servicios de la sociedad de la información, surge este derecho que permite al titular de los datos un mayor control de sus datos adaptado a este entorno; como se pone de manifiesto en el Considerando 6 del RGPD[319].

En sintonía con la STJUE y el RGPD, la LOPDGDD regula la materia, en principio remitiéndose al texto del RGPD, puntualizando que cuando la supresión de los datos se origine en el ejercicio del derecho de oposición, el responsable podrá mantener los datos necesarios para prevenir, subsanar o prevenir en el futuro el uso de los mismos con fines de mercadeo. También limita este derecho cuando este entra en conflicto con el ejercicio de la libertad de expresión, información, o cuando la supresión pueda afectar fines científicos, históricos o estadísticos, o bien cuando el ejercicio de este derecho se contraponga al interés público. Del mismo modo, se establece la obligación del responsable del tratamiento de responder a la solicitud de supresión en un plazo no mayor a un mes, y en caso de no aceptar la solicitud, deberá de hacerlo de manera fundada.

De esta forma, el RGPD integra a su texto el derecho al olvido en el artículo 17, y de la misma manera es recogido en la LOPDGDD en diversos artículos y en particular en el artículo 15; estableciendo que el responsable de los datos deberá suprimir los datos que el titular solicite, en el mínimo tiempo posible, siendo pasible de sanciones en caso de incumplimiento. En particular, se establece que los interesados tienen derecho a que sus datos sean suprimidos cuando los mismos hayan sido recabados sin su consentimiento o se haya suprimido el mismo, o cuando la causa para la que fueron recabados ya no existiera o cuando dichos datos ya no sean necesarios para la finalidad primaria.

El contenido del derecho al olvido se recoge en el art. 17 RGPD en dos apartados:

[319] "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial (…)".

1º) el derecho del interesado de obtener del responsable del tratamiento sin dilación indebida la supresión de los datos personales que le conciernen[320], cuando concurran las circunstancias previstas en sus apartados a) a f)[321].

2º) el segundo apartado del art. 17 contiene la obligación del responsable del tratamiento de "(…) *informar a los responsables que estén 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*", en el supuesto de que "(…) *haya hecho públicos los datos personales y esté obligado, 2.2.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 técnica".*

En la aplicación de este derecho, se va a poner de manifiesto, como hemos visto, su condición de ser un derecho limitado, resultando necesario proceder a ponderar los intereses en juego, como resulta del apartado 3 del art. 17; el cual excepciona la aplicación de los dos apartados anteriores, cuando en el tratamiento sea necesario, entre otros motivos:

"*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"*[322].

[320] Por tanto, se podrá ejercer más allá de los motores de búsqueda de Internet, como señala ÁLVAREZ CARO M., *op.cit*., p. 217

[321] "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".

[322] Otros motivos de inaplicación de los apartados 1 y 2 del art. 17 RGPD, serían:
"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;

El reconocimiento del derecho al olvido en el derecho positivo trajo consigo una gran novedad digna de resaltar reconociendo este derecho a las personas fallecidas. Dicho derecho podrá hacerse efectivo o bien a través de sus sucesores, o bien a través personas vinculadas al titular, siempre con sujeción a las instrucciones del fallecido, así como también través del "testamento digital" en lo que refiere a los datos proporcionados a prestadores de servicios de la sociedad de la información[323].

Este derecho resulta muy oportuno para los casos en que el consentimiento para la difusión de los datos fuera otorgado por menores de edad, que pueden ser inconvenientes o perjudiciales ante el cumplimiento de la mayoría.

Si trasladamos este derecho al ámbito sanitario, resulta relevante incluir los fundamentos de una sentencia de la Audiencia Nacional[324] que, revocando una resolución de la AEPD a la que el médico recurrió para solicitar su derecho de oposición, rechaza la petición del sanitario de solicitar a Google la retirada de un enlace que conectaba con un foro en el que un paciente le criticaba de forma muy negativa; concluyendo que Google no tendría que haber sido obligado a eliminar de sus resultados enlaces que lleven a contenidos de este tipo.

Pese a que se trataba de comentarios que fueron publicados varios años antes, el gestor del motor de búsqueda entendía que la accesibilidad a la información mediante el buscador "podía estar justificada por un interés superior al derecho individual a la protección de datos: el interés del público y de futuros pacientes en conocer las opiniones y experiencias personales de otros pacientes".

La sentencia fundamenta su decisión se basa en distintos motivos, como el carácter profesional por encima del personal -ya que los comentarios sólo afectan a la actividad profesional (no personal) del médico, que se trata de meras opiniones, que quedan al margen de la LOPD. Además, existe un interés general "legítimo de los internautas

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".

[323] DOPAZO FRAGUIO P., *op. cit.*, pp. 113-148.

[324] SAN de 11 de mayo de 2017 (recurso nº 30/2016).

potencialmente interesados en tener acceso a la información [...], pues al tratarse de un médico en activo, que presta servicios sanitarios privados, los usuarios o potenciales pacientes tienen derecho a conocer las experiencias y opiniones vertidas por quienes, con anterioridad, han sido pacientes de este mismo dolor".

Además, confluye un motivo de libertad, por cuanto el acceso a la información deviene lícita y protegida por la libertad de expresión.

2.2.1.5.1. Supresión de datos en la Historia Clínica

Como señala la AEPD, si nos situamos en el ámbito sanitario, la prohibición de tratamiento de datos especialmente protegidos se excepciona con un carácter muy restringido, en la medida que es necesario que los datos tratados se dediquen a fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia sanitaria o tratamiento sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social; o cuando el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a las amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y seguridad de la asistencia sanitaria y de los medicamentos y productos sanitarios. La concreción de los datos que deben suprimirse pertenece en exclusiva al profesional sanitario que atiende al paciente[325].

La HC puede tener utilización fuera de la finalidad asistencial en ámbitos como el judicial, epidemiológico, de investigación o docencia, relacionados con la garantía del interés público o el cumplimiento de obligaciones legales, por lo que la cancelación de los datos de la HC es excepcional. En este sentido, la cancelación de los datos innecesarios y no pertinentes puede resultar poco efectiva si nos situamos en el ámbito de la asistencia sanitaria, ante la necesidad de mantenimiento y conservación de los datos en situaciones específicas, como enfermedades crónicas e incurables, en los que en ningún caso desaparece la relación entre la finalidad perseguida que legitimó el tratamiento y el

[325] AEPD, Guía sobre protección de datos.

empleo de los datos sanitarios; además, en estos casos, los datos nunca se transformarían en impertinentes e inadecuados[326].

2.2.1.6. Derecho a la portabilidad de los datos

El RGPD (art. 20) ha venido a configurar un nuevo derecho para los usuarios que viene a complementar al derecho de acceso, al permitir a aquellos titulares de datos que los han suministrado a una empresa obtenerlos en un formato estructurado, de uso común y de lectura mecánica. Al mismo tiempo dichos datos podrán ser transmitidos directamente, sin pasar por el usuario, a otra empresa o a otro proveedor de servicios; además de que su titular pueda volverlos a obtener y reutilizarlos, por lo que su titular podrá bien descargarlos directamente o que los mismos se transmitan las empresas entre sí[327].

De esta forma, este derecho promueve el cambio entre proveedores de servicios y reforzar la competencia. Presupone un "refuerzo añadido al poder de disposición sobre los datos de las personas, así como una herramienta dirigida a fomentar la competencia dentro del mercado digital"[328]. Se manifiesta mediante la posibilidad de que los titulares de datos puedan obtenerlos de aquellas empresas a las que previamente se los hayan suministrado, utilizando un formato estructurado, de uso común y de lectura mecánica, pudiendo reutilizarlos posteriormente; al mismo tiempo, que los datos podrán transmitirse directamente (sin que tengan que ser entregados por el titular) de la entidad inicial a otra entidad distinta. Para el ejercicio de este derecho es preciso que se realice un tratamiento de forma automatizada que cuente con el consentimiento del afectado o exista un contrato previo.

Por tanto, el interesado tendrá derecho a recibir los datos personales que le incumban-siempre que no afecte a derechos y libertades de terceros- que haya facilitado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y a que sean transmitidos de forma directa -si es posible técnicamente- a otro responsable

[326] AEPD, Guía sobre protección de datos.
[327] AEPD,Comunicación de 16 de diciembre de 2018: https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-el-derecho-la-portabilidad
[328] FERNÁNDEZ-SAMANIEGO, J., y FERNÁNDEZ-LONGORIA, P., "El derecho a la portabilidad de los datos", en *El Reglamento General de Protección de datos…*, *op.cit.*, p. 273.

del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, requiriéndose: que el tratamiento esté basado en el consentimiento del afectado y que se lleve a cabo a través de medios mecanizados.

De acuerdo con las "Directrices sobre el derecho a la portabilidad de datos del Grupo de Autoridades europeas de Protección de Datos"[329], la finalidad de la portabilidad es "aumentar la capacidad de los usuarios de trasladar, copiar o transmitir sus datos personales fácilmente de un entorno informático a otro" al tiempo que se facilita el cambio de un proveedor de servicios a otro, lo que redunda en la competencia entre los servicios. Así mismo, pretende reforzar la competencia entre proveedores de servicios informáticos facilitando la posibilidad de cambiar de consumidores.

Se exceptúa el ejercicio de este derecho al propio derecho de oposición del afectado, así como 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[330].

Hay que destacar que "la portabilidad de los datos no conlleva el borrado de los datos de los sistemas del responsable del tratamiento ni afecta al periodo de retención o conservación informado al titular de los datos como aplicable a los datos que el mismo ha proporcionado"**.**

329 Aprobadas por el GT29,consistentes en varias directrices y documentos de preguntas frecuentes dirigidas a responsables y encargados de tratamiento de datos, adoptadas el 12 de enero de 2017.

330 Arts. 20 RGPD y 17 LOPDGDD.

Se incluye a continuación un cuadro descriptivo sobre la estructura y características de este derecho, siguiendo a su autor GONZÁLEZ LÓPEZ[331].

Definición	Objetivo	Elementos	Supuestos en que puede solicitarse	Datos que debe incluirse	Plazo de respuesta	Medio para la transmisión
El artículo 20 del Reglamento general de protección de datos (RGPD) crea un nuevo derecho a la portabilidad de los datos, estrechamente relacionado con el derecho de acceso aunque diferente de este en muchos aspectos. Permite a los interesados recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica y transmitirlos a otro responsable del tratamiento. El propósito de este nuevo derecho es capacitar al interesado y darle más control sobre los datos personales que le conciernen.	El objetivo primordial de la portabilidad de los datos es mejorar el control de los individuos sobre sus datos personales y garantizar que desempeñan un papel activo en el ecosistema de datos.	Derecho del interesado a recibir un subconjunto de datos personales que le conciernan, procesados por un responsable del tratamiento, y a almacenar dichos datos para un uso personal posterior.	Cuando las operaciones de tratamiento se basen en el consentimiento del interesado (con arreglo al artículo 6, apartado 1, letra a, o con arreglo al artículo 9, apartado 2, letra a, en el caso de categorías especiales de datos personales).	Datos personales que incumban a la persona solicitante.	Sin dilación indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud.	Deber llevarse a cabo en un formato que permita su reutilización, "en un formato estructurado, de uso común y lectura mecánica".
		Derecho a transmitir los datos de un responsable del tratamiento a otro responsable del tratamiento sin impedimentos.	Cuando las operaciones de tratamiento se basen en un contrato del que el interesado es parte, de conformidad con el artículo 6, apartado 1, letra b).	Datos que esta persona haya facilitado a un responsable del tratamiento.	El plazo de un mes puede ampliarse a un máximo de tres meses para los casos complejos, siempre que se haya informado al interesado de los motivos de dicho retraso en el plazo de un mes desde la solicitud original.	Cuando no existan formatos de uso común en un sector o contexto determinados, los responsables del tratamiento deben proporcionar los datos personales utilizando formatos abiertos de uso común (p. ej. XML, JSON, CSV) junto con metadatos útiles con el mejor nivel posible de granularidad, al tiempo que mantienen un alto grado de abstracción.
		Solo se deben aceptar y conservar los datos que sean necesarios y pertinentes para el servicio que preste el nuevo responsable del tratamiento.	El GDPR no establece un derecho general a la portabilidad de los datos para los casos en los que el tratamiento de datos personales no se base en el consentimiento o en un contrato.	Datos facilitados de forma activa y consciente por el interesado (por ejemplo, dirección postal, nombre de usuario, edad, etc.)	El artículo 12 prohíbe al responsable del tratamiento cobrar un canon por facilitar los datos personales, a menos que dicho responsable pueda demostrar que las solicitudes son manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo.	
		No limita el ejercicio de los demás derechos establecidos en el GDPR. La portabilidad de los datos no conlleva su supresión automática de los sistemas del responsable del tratamiento, ni afecta al periodo de retención original aplicable a los datos que se han transmitido.	El derecho a la portabilidad de los datos se aplica únicamente al tratamiento que se efectúe por medios automatizados y no incluye la mayor parte de los archivos en papel.	Datos observados facilitados por el interesado en virtud del uso del servicio o dispositivo. Estos pueden incluir, por ejemplo, el historial de búsqueda, los datos de tráfico y los datos de ubicación de una persona. Pueden incluir asimismo otros datos en bruto tales como el ritmo cardíaco registrado por un dispositivo ponible.		
			Si la transmisión de los datos de un responsable del tratamiento a otro impidiese a un tercero ejercer sus derechos como interesado en virtud del RGPD (tales como los derechos a la información, al acceso, etc.) no podrá llevarse a cabo el derecho de portabilidad.	Los datos inferidos y deducidos son aquellos creados por el responsable del tratamiento sobre la base de los datos "facilitados por el interesado", éstos no estarán dentro del alcance de este nuevo derecho.		

[331] GONZÁLEZ LÓPEZ, U., "El derecho a la portabilidad en el Reglamento General Europeo de Protección de Datos", *LegalToday*. Disponible en: http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-prodat/el-derecho-a-la-portabilidad-de-los-datos-en-el-reglamento-general-europeo-de-proteccion-de-datos

Situándonos en el ámbito sanitario, más en concreto en el biomédico, los ensayos clínicos en los que, normalmente se realizan en los hospitales y participan los propios pacientes del mismo como sujetos de estos ensayos, éstos tienen derecho a recibir información sobre el propio ensayo y transmitir los datos a otra organización.

Además, podríamos preguntarnos, cual es la repercusión de este nuevo derecho a la portabilidad sobre la historia clínica de los pacientes. A ello, podría responderse, tomando como referencia la Guía para el Ciudadano de la AEPD[332], señalando que este derecho sólo se aplicaría si los datos se están tratando como consecuencia de la existencia de un consentimiento de su titular o bien que existe un contrato previo; por tanto, es necesario que se dé una acción voluntaria del titular de los datos.

De lo anterior, puede concluirse que quedan excluidos de este derecho todos los datos que el SNS recoge de todas las personas como beneficiarias o aseguradas del mismo, sin que, por tanto, exista consentimiento previo; ya que, como sabemos, el tratamiento de datos con esta finalidad por las Administraciones sanitarias tiene su fundamento en el cumplimiento de una obligación legal o misión de interés público o en el ejercicio de poderes públicos[333].

2.2.1.7. Los nuevos Derechos Digitales que pueden afectar a los datos de salud

La LOPDGDD, además de adaptar a nuestro ordenamiento las prescripciones del RGPD, completando sus disposiciones, introduce como novedad la finalidad de dirigirse a garantizar los derechos digitales de los ciudadanos, de acuerdo con el Título X de la ley, arts. 79 a 97. Así, se reconoce el ejercicio de distintos derechos, que veremos a continuación, -y sobre alguno de los cuales la AEPD no tendrá competencias de actuación[334]-; los contenidos en los artículos 79 a 88 y 95 a 97. Son los llamados

[332] AEPD, Guía para el Ciudadano, 7 de febrero de 2019.
[333] Arts. 20.3 RGPD y 17 LOPDGDD.
[334] Por lo que será en el futuro desarrollo reglamentario de la ley en el que se determine en el organismo público competente.

"derechos de la Era digital": de neutralidad; de acceso universal, y rectificación en Internet; a la seguridad y educación digital; protección de menores en Internet; actualización de informaciones en medios de comunicación digitales; derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral; derecho a la desconexión digital en el ámbito laboral y los derechos de portabilidad en servicios de redes sociales y servicios equivalentes; testamento digital y políticas de impulso de los derechos digitales.

El preámbulo de la ley nos ayuda a situarnos en el contexto: "Internet se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva". Y, así, de esta forma "(…) *corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía".*

La regulación de estos derechos en la Ley que tienen una afectación con la salud es la siguiente:

1. Derechos generales de los ciudadanos en internet (arts. 79 a 82).

En este apartado, habría que considerar y valorar la red Internet. Así, la utilidad de la información volcada en la red es, sin duda, muy valiosa tanto para Administraciones sanitarias, profesionales sanitarios y pacientes. Sin embargo, esta información para ser válida y adecuada debe ser utilizada adecuadamente (partiendo de la proveniente de páginas oficiales), en la medida en que no toda ella proviene de fuentes fidedignas; lo que, por el contrario, puede constituir un auténtico riesgo en manos de personas que no sepan discriminara.

Además, Internet no sólo se utiliza como fuente de información documental, sino que también puede emplearse como espacio de información y comunicación conjunto o plataforma de interacción para mejorar las relaciones médico-paciente, compartiendo conocimientos y mejorando la comunicación entre ambos; al mismo tiempo que se podría mejorar la participación del paciente en la toma de decisiones que afectan a su salud.

Además, podría permitir que los pacientes accedan a su HC y permitir que puedan acceder a programas asistenciales y de promoción y prevención de la salud, que, sin duda, ayudarían a tener un paciente más informado para la toma de decisiones que le afectan.

a) Los derechos en la era digital (art. 79).

Como declaración general se establece que "*Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación".*

b) Derecho a la neutralidad en internet (art. 80)

Se reconoce a los usuarios de internet el "*derecho a la neutralidad de Internet*"; de forma que el contenido de este derecho se hará efectivo mediante la obligación de "(…) *los proveedores de servicios de Internet de proporcionar una oferta transparente de servicios sin discriminación por motivos técnicos o económicos*".

c) Derecho de acceso a internet y brecha de género (art. 81)

Seguramente se trate de una de las novedades de mayor incidencia social consistente en el derecho de todos al acceso a internet, como un derecho universal, asequible, de calidad y no discriminatorio para la población, que tenga en consideración a las personas con necesidades especiales. Además, este acceso procurará la superación de las brechas de género y generacional, considerando el entorno rural.

Por algún autor se ha puesto de manifiesto la necesidad de que la CE reconociera el acceso universal a internet como nuevo derecho fundamental y la consideración de su neutralidad como principio general del Derecho de internet[335].

d) Derecho a la seguridad digital (art. 82)

Reconoce el derecho de que "*Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet*"; que, igualmente, se

[335] BARRIO ANDRÉS, M., "Fundamentos del Derecho de Internet", *Centro de Estudios Políticos y Constitucionales,* Madrid, 2017, pp. 267 y ss.

llevará a cabo por los proveedores de servicios de Internet mediante la información a los usuarios de sus derechos.

2. Derechos relacionados con el ámbito laboral (arts. 87 a 91)[336]

En este apartado examinamos aquellos derechos que se ven afectados por la salud laboral:

a) Derecho a la desconexión digital en el ámbito laboral (art. 88)

Estamos ante un derecho reconocido en otros países, destinado a "potenciar el derecho a la conciliación de la actividad laboral y la vida personal y familiar", mediante el "respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar".

La incidencia de este derecho sobre la salud laboral es evidente: La continua conexión laboral del empleado no sólo mina la productividad, sino que tiene efectos directos negativos sobre su salud, equiparables a los del estrés laboral.

3. Derecho al olvido en internet (arts.93 y 94)

Como complemento de lo examinado anteriormente en el apartado vi), podemos ver como la ley diferencia o separa el derecho de supresión o derecho al olvido[337] en dos áreas:

a) En los motores de búsqueda, "*Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran 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…"; y*

[336] Para más información, Vide AEPD, Guía sobre la protección de datos en las relaciones laborales, 4 marzo 2014.
[337] Regulado en el art. 17 RGPD y 15 LOPDGDD.

b) En las redes sociales "*Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes".*

Como vimos anteriormente para la aplicación del derecho al olvido en el campo de la salud, en el caso de la utilización de Internet, partiendo de los postulados de la STJUE de 13 de mayo de 2014, los pacientes o usuarios de la salud pueden hacer comentarios lesivos en redes sociales o en blogs de opinión sobre resultados de tratamientos médicos en contra de los profesionales sanitarios, que pueden perjudicar su imagen profesional. Ante lo cual, estos profesionales pueden solicitar la eliminación de sus datos identificativos, en la medida en que prevalece su derecho a la privacidad sobre un pretendido derecho a la información o libertad de expresión.

2.2.2. EJERCICIO DE LOS DERECHOS DEL PACIENTE FRENTE AL TRATAMIENTO DE DATOS DE SALUD

2.2.2.1. La Historia Clínica (HC): HC digital

i) Contenido y finalidad

El acceso a los datos personales por su titular en el ámbito sanitario-asistencial lo centramos en la HC. Veremos las particularidades del acceso a la misma; tanto por el propio paciente, como por profesionales sanitarios y no sanitarios, además del acceso por terceros.

La HC está constituida por un conjunto de información, dinámico, en permanente actualización, no solamente de contenido sanitario, sino que además incluye una variada información complementaria. Toda esta información de especial trascendencia y sensibilidad, integra un documento unitario (principio de HC única)[338] en el que se refleja

[338] El art. 14 de la LBAP, la define como: "(…) el conjunto de los documentos 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". Su contenido mínimo es que se regula en el art. 15.2 de la LBAP.

la práctica o acto médicos[339], junto al cumplimiento de distintos deberes del profesional sanitario con el paciente, como el de asistencia, información y constancia del consentimiento[340], con la prioridad del uso asistencial de paciente[341]; todo lo cual justifica la necesidad de un régimen de especial protección.

No olvidemos que, además de elemento esencial en la asistencia sanitaria, en el ámbito judicial, constituye un importante documento probatorio de la práctica clínica realizada por los profesionales sanitarios, convirtiéndose, al mismo tiempo, en un elemento fundamental de defensa de su actuación profesional. Así, la importancia de recoger en la HC todo el proceso asistencial del paciente en cuanto tenga repercusión en su enfermedad. Siendo fundamental incluir la prestación de la información al paciente y el posterior consentimiento del mismo, previos a cualquier actuación sanitaria.

En este sentido, El GT29 señalaba que, por un lado, no sirve la mera "utilidad" para justificar la inclusión de datos en la HC, y que, además,

"(...) la exhaustividad de un expediente médico es prácticamente imposible y tampoco deseable, por lo que solamente debe introducirse en la HCE la información relevante", es decir, "según los principios de pertenencia y proporcionalidad de la recopilación de datos, toda compilación de datos debe limitarse a aquellos datos que sean adecuados, pertinentes y no excesivos con relación a los fines que se recaben y para los que se traten posteriormente (art. 6.1.c) Directiva 95/46/CE"[342].

[339] En una reciente sentencia del 2019 del TSJ de Andalucía, el tribunal, sobre la necesidad de colegiación de los inspectores médicos al servicio de la Junta de Andalucía, acoge el concepto de acto médico acuñado por Ricardo de Lorenzo, en Redacción Médica, 3 de abril de 2019, que señalaba que: "puede entenderse en un doble punto de vista: no basta con que sea un acto subjetivamente médico, sino también objetivamente médico, es decir, sobre el hombre y para el hombre y con el ánimo de prevenir, curar, aliviar o rehabilitar al hombre ante el acoso y riesgo de enfermedad… La actividad médica, en cuanto conjunto o sucesión de actos médicos, no opera sólo en el campo biológico humano, sino que se desarrolla dentro de unas coordinadas jurídicas y con unos efectos jurídicos".
Para más información, vide DE LORENZO Y MONTERO, R., *Protección de datos personales en el sector sanitario*, Edit. Colex, La Coruña, 2009.

[340] SARRATO MARTÍNEZ, L., "*Revista Jurídica de Castilla y León*", nº 17, enero 2019, p.181.

[341] Art. 16 de la LBAP.

[342] "Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos". Disponible en: http://europa.eu.int/comm/justice home/fsj/privacy/index en.h.

La HC forma parte de la historia personal del paciente, siendo su finalidad fundamental la asistencia del paciente, a cuyo efecto, su contenido[343] "incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente". La HC integra un derecho y un deber: el derecho del paciente a que "quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada"[344]; y el deber-obligación del profesional sanitario de redactar y elaborar la HC de todo paciente que sea atendido, haciendo constar todos los datos que reflejen su estado de salud[345].

ii) La Historia Clínica como portador esencial de datos sanitarios

La HC como elemento fundamental de la documentación clínica-sanitaria está sujeta a la interacción de una doble normativa: a) como fichero[346] individual de datos, comprensivo de datos personales, ha de estar sometido a la normativa reguladora de la protección de datos personales, que hemos enunciado anteriormente; y b) como elemento fundamental de la asistencia sanitaria debe acomodarse a la normativa específica propia de este ámbito: básicamente la LBAP, LGS, LOPS[347], Código Deontológico Médico, de julio de 2011;

[343] El contenido mínimo de la HC se establece en el art. 15.2 LBAP. De hecho, la mayoría de las CCAA lo han ampliado a través de sus leyes sectoriales.
[344] Art. 15.1 LBAP.
[345] En aplicación de lo dispuesto en el art. 2.6 LBAP.
[346] Se denomina fichero: "Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica" (art. 4.6 del RGPD).
[347] Ley 44/2003, de 21 de noviembre, de Ordenación de las profesiones sanitarias.

además de la normativa administrativa reguladora del Servicio Regional de Salud correspondiente[348], y de la regulación contenida en el Código Penal[349].

Actualmente, habida cuenta de la gestión de la asistencia sanitaria por equipos multiprofesionales, nos encontramos ante una historia clínica compartida, en cuyo contenido inciden actuaciones de diferentes profesionales de la salud, tanto propios de profesiones y técnicos sanitarios, como personal de gestión administrativa; como veremos en el apartado del acceso a al HC. De esta forma, estamos ante un documento (tanto en papel como digital) en el que la protección del derecho a la confidencialidad de los datos del paciente cobra mayor dificultad, ante la diversidad de profesionales sanitarios y no sanitarios que intervienen en el proceso asistencial del paciente, además de otros posibles accesos regulados legalmente.

iii) Historia Clínica Digital (HCD): problemática en cuanto a la protección de datos

El GT29[350] se refería a la HCD como *"(...) un historial médico completo o una documentación similar del estado de salud físico y mental, pasado y presente de un individuo, en formato electrónico, que permite acceder fácilmente a estos datos a efectos de tratamientos médicos y otros fines estrechamente relacionados".* En esta definición deberíamos entender incluidos los datos propios de los profesionales sanitarios.

[348] El Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, establece que "(…) las comunidades autónomas podrán establecer sus respectivos modelos de documentos clínicos, incorporando aquellas otras variables que consideren apropiadas. Dichos modelos deberán incluir, en todo caso, todas las variables que integran el conjunto mínimo de datos, tal y como figuran en los anexos de este real decreto (…)" (art. 3).
A modo de ejemplo, en la Comunidad de Madrid, Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria, junto al Decreto 24/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece el régimen jurídico y de funcionamiento del Servicio Madrileño de Salud.
Por su parte, el País Vasco, ha dictado como norma específica 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.

[349] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en su rúbrica del delito de "descubrimiento y revelación de secretos", del capítulo I, del Título X, denominado "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio".

[350] GT29 Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos, 00323/07/ES. WP 131, de 15 de febrero de 2007.

La HCD añade un soporte nuevo a la historia clínica manual, pero sin destruir su concepción básica; aunque, lógicamente, añade una problemática diferente, derivada del propio soporte utilizado[351].

Como señala la AEPD, "La HCD o Historia clínica electrónica (HCE) supone utilizar las TICs en la actividad sanitaria, almacenando la información generada de forma digital, facilitando su integración en un Sistema de Información Clínica, normalmente denominado HIS (*Healthcare Information Systems*). Sería como la versión digital de la HC, comprensiva de una registro unificado y personal, de contenido multimedia, archivado en soporte electrónico"[352].

El devenir de la HC, supone haber pasado de una HC en documento papel a la HC digitalizada, a la que se han incorporado las últimas tecnologías de información y comunicación (TICs), con lo que se consigue integrar activamente y de forma continuada, ordenada y precisa en un único documento –único para cada paciente- todos los actos médico-sanitarios que integran el proceso asistencial del paciente (tanto los informes propiamente clínicos como los resultados de las distintas pruebas prescritas[353]), con inmediata disponibilidad a la hora de acceder a su contenido; lo que permite una mayor calidad y seguridad en la atención médica.

Sin embargo, el hecho de que la digitalización permita tratar una mayor cantidad de datos personales permite al mismo tiempo una mayor utilización o accesibilidad para un número mayor de destinatarios (como veremos seguidamente), lo que supone un riesgo potencial elevado y, por tanto, una mayor necesidad de medidas preventivas y de seguridad activas y pasivas.

En este sentido, el GT29[354] se refería a la necesidad de incorporar un contrapeso a favor de los pacientes dirigido a preservar su intimidad en distintas situaciones, así como el principio de autodeterminación o de autonomía. Así (apartado III.1), de forma no

[351] SÁNCHEZ-CARO, J., "Principios de la protección de datos: el uso y acceso a la historia clínica electrónica (HCE) y la protección de datos", en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, op.cit*., pp. 1058-1080.

[352] AEPD. Plan de inspección sectorial de oficio en Hospitales públicos. 2017, pp. 7 y ss.

[353] La SAN de 6 de noviembre de 2013, considera que las imágenes o placas de las pruebas médicas (radiografías y demás pruebas diagnósticas de imagen) forman parte de la historia clínica, a efectos de la normativa de protección de datos.

[354] Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos, *op.cit*.

asimilable al consentimiento informado, se refería al "acuerdo" del paciente al acceso a sus datos personales, que supondría una especie de consulta previa para determinados datos sanitarios, especialmente íntimos, como serían los datos psiquiátricos, para los que cabría exigir un consentimiento previo y expreso del paciente, y los de abortos, en los que podría reconocerse al paciente la posibilidad de denegar el acceso a un profesional para un momento concreto[355].

Partiendo de los principios de unicidad e integridad de la HC, se ha articulado un sistema de compatibilidad en el acceso a la información, con actuación coordinada y compartida entre el Estado (como responsable) y las Comunidades Autónomas (como ejecutoras), que ha dado lugar a la implantación de la Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS), en cuyo proceso ha jugado un papel importante la tarjeta sanitaria y la configuración de un número o código de identificación personal y único para todo el ámbito del SNS, que permite acceder a la información de un paciente desplazado fuera de su Comunidad de residencia.

La HCDSNS, permite el acceso, exclusivamente con fines asistenciales, a la HC del paciente, elaborada en cualquier Servicio Regional de Salud, y tiene como finalidad garantizar a ciudadanos y profesionales sanitarios el acceso a la documentación clínica más relevante para la atención sanitaria de cada paciente.

Se incluye en ella documentación que se encuentre disponible en soporte electrónico en cualquier lugar del ámbito del SNS, y se pretende satisfacer las necesidades médicas de los ciudadanos en sus desplazamientos por el territorio nacional y las de los profesionales de todo el SNS que tienen responsabilidades en su atención; haciendo posible que los datos básicos de los ciudadanos que necesiten asistencia sanitaria fuera de su Comunidad Autónoma sean accesibles para los profesionales sanitarios que necesiten atender al paciente, disponiendo de la tecnología y la información necesaria que garantice la mejor asistencia sanitaria posible en condiciones de igualdad efectiva en cualquier Centro sanitario del SNS[356].

[355] Quizás podría añadirse a estos datos sanitarios diferenciados, los datos genéticos, los incluidos en las técnicas de reproducción humana asistida, los de VIH, trasplante de órganos, etc.
[356] Art. 56 de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

Los documentos electrónicos a los que se puede acceder mediante la HCDSNS son los siguientes:

Historia Clínica Resumida (HCR); Informe de Atención Primaria; Informe Clínico de Urgencias; Informe Clínico de Alta; Informe Clínico de Consulta Externa de Especialidades; Informe de Cuidados de Enfermería; Informe de Resultados de Pruebas de Laboratorio; Informe de Resultados de Pruebas de Imagen; Informe de Resultados de otras Pruebas Diagnósticas. Todos estos documentos electrónicos (excepto la HCR) constituyen informes clínicos incorporados a la HC del paciente; de forma que no pueden ser modificados por un profesional médico de otra Comunidad Autónoma que accede al sistema de HCDSNS.

La HCR está integrada por los datos que se incorporan "ex novo" automáticamente a partir de la HCE del paciente, con el contenido mínimo necesario que permita disponer de la información básica al profesional médico que atiende por primera vez al paciente. Por cada paciente y Comunidad Autónoma existirá una HCR derivada de su HCE, que sólo incluirá las modificaciones producidas en ésta última; existiendo un acceso centralizado a todas las existentes mediante un punto de acceso del Ministerio de Sanidad.

En relación con las modalidades de organización de los sistemas de HCD, tanto centralizado como descentralizado, el GT29, se refería a la modalidad de almacenamiento centralizado, en el que los profesionales sanitarios vuelcan su documentación en el Sistema general, permitiendo, a su vez, que profesionales distintos puedan acceder a la HCD; señalando que, aunque respeta la autodeterminación, puede plantear problemas en cuanto a la calidad de los datos si fuera el caso de que el interesado decidiera los datos que se guardan en su HC y, sobre todo, si no se recoge la intervención de un profesional médico. Por ello, entiende que, no obstante, la mejor opción es el almacenamiento centralizado, dotado de mayor disponibilidad y seguridad técnica, y que permite un acceso permanente. Sin embargo, este sistema desde la óptica de la protección de datos podría tener el inconveniente de su vulnerabilidad ante una mayor posibilidad de uso ilícito, lo que podría limitarse mediante medidas preventivas y de seguridad, que, no obstante, ahora se recogen en el RGPD, como veremos.

Actualmente, los distintos documentos-informe que componen la HCD[357] se encuentran en fase de adaptación progresiva en todas las CCAA; habiendo finalizado el proceso en Atención Primaria[358]. El documento correspondiente a la HC resumida únicamente se encuentra pendiente de implantar en Madrid y Asturias. Con la incorporación de Cataluña, en enero de 2019, la historia clínica electrónica ya es interoperable, y su extensión completa está prevista para el este año; con ello, los profesionales sanitarios, debidamente autorizados y los pacientes podrán consultar la información clínica normalizada existente en cualquier servicio autonómico de salud[359].

2.2.2.2. Acceso a los datos de salud

En el apartado 2 anterior nos hemos referido a los derechos de los titulares de datos y a su ejercicio por su titular, el cual dispone de un poder de control sobre los mismos, que se materializa a través del ejercicio de distintos derechos; entre los que se encuentra el derecho de acceso frente al responsable del fichero de los datos, que en este caso se trata del director de un centro o establecimiento de carácter sanitario.

A partir de la STC 254/1993, se considera que el derecho de acceso constituye un aspecto nuclear del derecho del interesado a la protección de sus datos personales[360]. El art. 15 RGPD, al que remite el art. 13 de la LOPDGDD, contempla el derecho de acceso de acceso, a través del "(…) *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 (…)*"; por lo que, el acceso abarca además a distintos aspectos de la información relacionada con el tratamiento. Además, el titular de los datos podrá solicitar copia de los datos que son objeto de ello.

[357] La HCD estará integrada por la historia clínica resumida, los informes de atención primaria, los informes de urgencias, los informes de alta y consulta, el informe de cuidados de enfermería, los datos de laboratorio, pruebas diagnósticas y demás pruebas.
[358] Ministerio de Sanidad, Consumo y Seguridad Social: https://www.mscbs.gob.es/profesionales/hcdsns/contenidoDoc/home.htm...
[359] Diario Médico, 3 enero 2019. https://www.diariomedico.com/tecnologia/la-historia-clinica-electronica-interoperable-al-fin-entre-todas-las-autonomias-tras-sumarse-cataluna.html.
[360] TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio*, *op.cit.*, pp. 111 y ss.

El derecho de acceso constituye un derecho con una finalidad instrumental dirigida a que el interesado pueda verificar la licitud del tratamiento, además de la posibilidad de ejercitar los derechos reconocidos en los arts. 16 a 22 del RGPD[361].

Estamos ante un mecanismo que habilita al interesado para poder ejercer el control de sus datos personales; ya que puede suceder que la persona acceda a sus datos personales con otras finalidades, en cuyo caso no está ejerciendo este derecho, sino otro distinto que pueda concederle el ordenamiento jurídico, distinto del derecho de acceso[362].

Los datos de salud que integran la HC son datos sensibles que reflejan un aspecto del ámbito de la intimidad de la persona, que han de ser preservados de forma confidencial; de ahí que se hable del derecho a la confidencialidad de la HC, cuyo acceso sin previa autorización del titular constituye una invasión de la dignidad humana (art. 10 CE), además de poder afectar a otros derechos fundamentales[363]. En este sentido, el TC haciéndose eco de la doctrina del TEDH, ha considerado que la protección de la información personal del paciente forma parte del respecto a la vida privada y familiar[364].

Como veíamos, en el acceso a los datos de salud van a incidir dos tipos de normativas, la propia del ámbito sanitario o de salud y la relativa a la protección de datos personales; las cuales habrán de conciliarse para hacer efectiva la prestación sanitaria, para lo que habrán de considerarse la aplicación de distintos principios, como el de vinculación asistencial con el paciente, el de proporcionalidad y el de autonomía, como veremos[365].

---

361 STJUE de 12 de diciembre de 2013, C-486/12, *Proceedings brought by X*.

362 HERNÁNDEZ CORCHETE, J.A.,"Transparencia en la información al interesado del tratamiento de sus datos personales", en *Reglamento General de Protección de Datos…, op.cit.,* pp. 223 y ss.

363 En este sentido, el art. 7.1 de la LBAP establece: 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.
Además, "La dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica" (art. 2.1. LBAP).

364 STC 159/2009 de 29 de junio (FJ 3).

365 Ejemplos de resoluciones sancionadoras de la AEPD por denegación indebida a un historial clínica, las encontramos en la Resolución R/01461/2010, por falta de atención por una clínica de estética de la solicitud de acceso de una paciente a su historia clínica. O, bien la Resolución sancionadora R/01627/2012 a un profesional médico por no permitir el acceso a la historia clínica de su paciente. Sobre la gratuidad en el ejercicio del derecho de acceso ver AEPD, informe 0437/2012.

i) Derecho de acceso. Conflicto entre accesibilidad y protección de la Historia Clínica

No debemos olvidar que nos encontramos en un ámbito muy específico y especialmente sensible: la asistencia sanitaria o la salud pública. En este terreno, el bien protegido evidentemente es la salud del paciente o de los ciudadanos, a cuyo tratamiento deben dirigirse preferencialmente todas las actuaciones sanitarias. No obstante, la atención sanitaria con ser prioritaria no puede desconocer la existencia de otros derechos que al mismo tiempo que se lleva a cabo inciden sobre una actuación de contenido médico. Así, la HC como instrumento fundamental en el proceso asistencial del paciente integra en su contenido un conjunto de datos sensibles a los que pueden acceder distintos profesionales sanitarios y no sanitarios, que están obligados a respetar su confidencialidad. En este sentido, las distintas cautelas o no autorizaciones de acceso existentes a fin de proteger los datos sanitarios contra accesos indebidos deben establecerse de forma equilibrada, ponderando en cada caso los intereses que están en juego, sin menoscabar o entorpecer en ningún caso la normal prestación de la asistencia sanitaria.

Los deberes de seguridad y secreto aplicables a los distintos tipos de acceso a la HC (que veremos a continuación) se completan para el ámbito sanitario con lo previsto en la LBAP, cuyo art. 16.6, sujeta al deber de secreto al personal que accede a los datos de la HC, y se refuerza con el deber de seguridad exigible a las CCAA y a los centros sanitarios al establecer que "las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y su uso" (art. 16.7).

Por tanto, podemos encontrarnos con la posibilidad de distintos problemas derivados de la aplicación de la normativa sobre protección de datos con motivo de su aplicación en el ámbito de la salud, derivados de la legislación existente ya comentada. Podemos señalar al respecto distintos casos:

a) En relación con el consentimiento expreso e inequívoco del paciente exigido por la normativa de protección de datos, supone un punto de fricción con la normativa sanitaria, ya que la LBAP exige con carácter general el consentimiento verbal del paciente (salvo para situaciones de cierto riesgo), puesto que, de exigirse el consentimiento expreso en general se burocratizaría y entorpecería la asistencia sanitaria.

b) En relación con el nivel de protección, tratándose de la cita previa de una persona en un centro sanitario, habría que articular la máxima protección a fin de proteger los datos

íntimos de los pacientes. Por ejemplo, no sólo a través de códigos numéricos identificables de cada persona, sino de agrupar a personas con una misma patología específica como el VIH en una planta o sala concreta, y procedimientos específicos de llamada a consulta al paciente en cuestión.

Dado que estamos tan afectados por la pandemia del COVID-19, se impone incluir, sin perjuicio de un desarrollo más amplio en otro epígrafe, alguna medida como, la utilización de la geolocalización de dispositivos mediante datos ofrecidos por las operadoras de telecomunicaciones de forma anónima y agregada, dirigida a conocer la movilidad geográfica de las personas, o la creación de aplicaciones (*apps*) que facilitan información sobre el Covid19 y permiten la autoevaluación del estado de salud personal (a veces, unido a la geolocalización individual). Pese a que los dispositivos manejan sólo variables anonimizadas, sin ninguna relación con personas físicas determinadas o determinables, las susceptibilidades o temores de invasión en la privacidad personal están siendo muy abundantes, lo que, sin duda, pone en peligro su utilización masiva, que es la clave del éxito de estos dispositivos. Quizás, si las Administraciones sanitarias hicieran más hincapié en promover campañas explicativas y divulgativas de estas técnicas, podrían eliminarse esos temores.

Incluso, en el acceso del paciente a la asistencia sanitaria, nos encontramos con que es muy frecuente que el Servicio de admisión del centro sanitario no compruebe la identidad de quien solicita el acceso mediante la comparación de la tarjeta sanitaria con el DNI, por lo que, es posible -aunque ciertamente infrecuente- que se produzcan casos de suplantación de identidad, que implicarían una importante distorsión en el sistema sanitario y en el propio paciente atendido al no existir correspondencia de los datos que figuran en su HC.

c) La cancelación de los datos personales cuando resultaran inexactos o excesivos, con carácter general, choca con las necesidades propias de la asistencia sanitaria de mantener las historias clínicas hasta un plazo de cinco años, aunque superior en algunas CCAA.

d) Tratándose de una cuestión frecuente en el ámbito sanitario[366], como es la atención sanitaria en un centro sanitario distinto al que inicialmente ha atendido al paciente,

[366] Recordemos, por ejemplo, que la Comunidad de Madrid tiene regulada la libertad de elección de Centro sanitario por Ley 6/2009, de 16 de noviembre.

derivada de procesos asistenciales que necesitan una segunda opinión o una mejor atención sanitaria que no puede prestarse en el primer centro, podría entorpecerse la asistencia sanitaria si no se realiza una interpretación flexible de la normativa sobre protección de datos.

ii) Acceso de pacientes/usuarios a su Historia Clínica

El paciente o usuario tiene derecho a dirigirse a su médico o centro de salud, como responsable del tratamiento de sus datos solicitando poder acceder al conjunto de documentos que integran su HC, bien estén comprendidos en la HCE o en formato papel. De forma que, por parte del responsable del tratamiento deberá informarle de si sus datos personales son objeto de tratamiento, en cuyo caso podrá acceder a los mismos y, además de facilitarle copia de los datos tratados, deberá ser informado de los siguientes contenidos:

Los fines del tratamiento; plazo de conservación; posibilidad de solicitar su rectificación, supresión, limitación u oposición del tratamiento; posibilidad de presentar reclamación ante la autoridad de control, en su caso, la existencia de decisiones automatizadas incluida la elaboración de perfiles; y sobre el origen datos personales no aportados por el interesado.

El paciente tiene derecho al acceso de su HC y a obtener copia de la misma; sin que pueda ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en la historia clínica, recogidos en interés terapéutico de la persona paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración; quienes pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas. Este derecho excluye el acceso a datos que deban limitarse por la existencia acreditada de un estado de necesidad terapéutica, del que el médico dejará constancia en la historia clínica[367].

[367] Art. 12 del 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, en relación con el art. 18 de la LBAP.

A la vista de esta regulación pueden señalarse la existencia de las siguientes limitaciones al acceso a la HC:

a) La existencia de una necesidad terapéutica del paciente que limite todos o algunos de los datos de la HC, reflejando el motivo de esta limitación, que no es necesario que se trate de enfermedades graves;

b) No es posible que en base al interés terapéutico del paciente éste acceda a datos confidenciales de terceros;

c) Las anotaciones subjetivas puestas por el profesional médico no son accesibles al paciente.

En las solicitudes de acceso a la documentación clínica de cada persona como paciente será necesario en todo caso "(…) *identificar adecuadamente a quien lo solicita, la información demandada, el motivo y finalidad de la solicitud, y la constancia de consentimiento expreso del paciente para que pueda producirse tal tratamiento de sus datos, sin perjuicio de las excepciones que contempla este Decreto. En la entrega o envío de la documentación se tomarán las medidas oportunas para salvaguardar la confidencialidad de la información proporcionada, quedando constancia de la documentación entregada*".

El acceso de la persona del paciente podrá realizarse por representación acreditada del paciente. En el supuesto de menores de 16 años no emancipados será necesaria la autorización de sus padres o representantes legales. Tratándose de pacientes incapacitados judicialmente corresponde al representante legal nombrar a la persona que pueda acceder a la HC[368].

[368] Art. 12.6. del Decreto 38/2012, de 13 de marzo.
Para más información sobre el acceso a la HC, Vide DE MIGUEL SÁNCHEZ, N., "Intimidad e historia clínica en la nueva la Ley 41/2002, de 14 de noviembre, básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica", *Revista española de Derecho administrativo*, nº 117, 2003

Salvo que una ley lo prevea expresamente, el derecho de acceso no incluye identificar los profesionales sanitarios que acceden a su HC como consecuencia de su proceso asistencial.

iii) Acceso a la Historia Cínica por los profesionales sanitarios con fines asistenciales

Como decíamos, el acceso[369] deberá tener en consideración el principio de la vinculación asistencial con el paciente y el principio de proporcionalidad, el cual será de aplicación a los accesos a la HCD para fines no asistenciales. Además, en el ámbito de la salud laboral, la aplicación de la Ley 31/1995, de prevención de riesgos laborales, establece que los datos relativos a la vigilancia de la salud de los trabajadores sólo serán accesibles al personal médico y a las autoridades sanitarias encargadas de la vigilancia de la salud, sin que pueda extenderse a otras personas, salvo consentimiento expreso del afectado.

El acceso a la HC, como variante del tratamiento de datos personales deberá ajustarse, además a lo previsto en la LBAP, artículo 16.1[370]. Así, tratándose de un instrumento destinado básicamente a la asistencia sanitaria al paciente, se justifica el acceso a la misma por parte de los profesionales sanitarios vinculados a dicho proceso asistencial, que, por tanto, participen en ese momento en el tratamiento del paciente, debiendo existir una relación de tratamiento médico real y actual entre el paciente y el profesional sanitario[371]; excluyendo que otros profesionales sanitarios con finalidades distintas (administrativas, investigadoras, etc.) puedan acceder válidamente a la misma, sin consentimiento expreso[372] del afectado, incurriendo, por ello, en un acceso indebido al violar la intimidad

[369] Para TRONCOSO REIGADA, A., "La protección de datos sanitarios: La confidencialidad de la historia clínica, Protección de datos personales para servicios sanitarios públicos", *Op.cit.*, pp.104 y ss., se habla de acceso autorizado a la historia clínica si ésta se encuentra centralizada, mientras se trataría de una cesión si se encuentra descentralizada.

[370] 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 (apdo.1).

[371] No sólo se incluyen a los médicos, en general, sino enfermeros, técnicos sanitarios y demás profesionales sanitarios. Además, debe incluirse al personal que presta servicios en la Administración Sanitaria (Servicios Regionales de Salud).
Como señala el apartado 2 del art. 16 LBAP, corresponde a cada centro sanitario establecer los métodos de acceso a la HC por los profesionales que asisten al paciente.

[372] Conforme a la SAN de 24 de marzo de 2006, debe entenderse por consentimiento expreso "aquel que se obtiene de una declaración clara e inequívoca por parte del interesado, que acepta o rechaza la cesión o uso de sus datos mediante la expresión de su voluntad de forma que permita su constancia y prueba indubitada. La existencia de consentimiento expreso, referido a la cesión y uso de estos datos especialmente

del paciente, subsumible en el tipo penal agravado del art. 199.2 del Código Penal, de delito de descubrimiento de secretos, para el que no se exige que exista un perjuicio para un tercero, ya que el delito se consuma por el mero acceso de los datos contenidos en la HC[373].

Por tanto, estamos ante la finalidad de la prevención, diagnóstico y asistencia sanitaria de los pacientes a quienes afectan los datos, por lo que no puede calificarse como una cesión o comunicación de datos, sino de un acceso legitimado por la exclusiva finalidad asistencial al paciente. Así, estos profesionales sanitarios podrán acceder a la HC, como excepción prevista en la LBAP a la prohibición general de tratamiento de estos datos[374], que exige el consentimiento expreso del afectado. Esta excepción debe ser interpretada restrictivamente[375]: el acceso habrá de ser concreto y proporcional o estrictamente necesario para cumplir con la finalidad para la que se accede, sin que pueda utilizarse para finalidades distintas[376].

iv) Acceso por terceros a la Historia Clínica

Junto al acceso por el propio interesado como parte esencial de su facultad de control sobre sus datos personales (derecho de acceso a su HC y a obtener copia de la misma)[377], como hemos visto, así como al acceso por familiares, allegados y representantes legales

sensibles, no debe admitir duda ni entenderse o interpretarse en varios sentidos o poder dar ocasión a juicios diversos".

373 Como señala la STS 1328/2009, de 30 de diciembre, ya que en los denominados "datos sensibles" su violación lleva implícito el perjuicio exigido.
La SAP de Navarra, de 3 de abril de 2017, se condena a una enfermera del Servicio Navarro de Salud por un delito continuado de descubrimiento de secreto, al haber accedido reiteradamente sin justificación asistencial y sin su consentimiento a la historia clínica de su expareja, pareja y hermano; sin que, como señala la sentencia, las relaciones anteriores con los afectados justifiquen los accesos indebidos, "(…) dado el carácter personalísimo del derecho a la libertad informática de cada uno de ellos (…)".

374 Conforme al art. 9.2. del RGPD.

375 AEPD, informe 0341/2009.

376 El art. 91.3 del derogado Reglamento de la Ley de Protección de Datos establecía la obligación del responsable del fichero de adoptar las medidas necesarias para evitar que un profesional acceda a recursos distintos a los autorizados, lo que, en aplicación del art. 89 de dicho Reglamento, implica que el responsable del centro identifique y defina las funciones y obligaciones de los distintos profesionales del centro, determinando por tanto las autorizaciones concretas de acceso a los datos de salud.

377 STSJ Madrid, Sala de lo Contencioso Administrativo, Sección 9ª, de 28 de febrero de 2006, que señala que: "no existe ningún obstáculo en que pueda proporcionarse al paciente copia de las diversas pruebas diagnósticas practicas (…)".

(previsto en la LBAP[378], así como en el Código de Deontología Médica[379]), la LBAP se refiere a otros usos de la HC distintos de los asistenciales, que habrán de adecuarse al principio de proporcionalidad en la información suministrada, quedando estrictamente limitados a los fines previstos para cada caso concreto y con el ámbito estrictamente necesario para el cumplimiento de dichos fines[380]. Además, a fin de que el acceso mantenga un cierto equilibrio entre los diferentes intereses afectados, que, de otro modo, podrían ver como se afecta su intimidad personal, la ley[381] obliga a que no se perjudiquen estos intereses, tanto de terceras personas como de los propios profesionales sanitarios que intervienen en la redacción de la HC.

En el acceso a la HC, quedará a salvo el derecho del profesional sanitario a oponerse a que se acceda a sus anotaciones subjetivas[382]; lo que implica que éstas se supriman del contenido del acceso, pero no que no se pueda entregar el documento en el que se contienen[383]. Esta objeción, alineada con la proporcionalidad de los datos suministrados, deberá ser planteada, en su caso, únicamente por el profesional sanitario no por el centro sanitario[384].

En este sentido, recientemente, ha aparecido información en la que se da a conocer que una compañía sanitaria de EE.UU. tiene almacenados historiales completos de pacientes, que incluyen diagnósticos médicos, resultados de pruebas y registros sanitarios, etc., siendo lo más inquietante que ni los propios pacientes titulares de los datos ni las

[378] Art. 5.1. "El titular del derecho a la información es el paciente. También serán informadas las personas vinculadas a él, por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita".
Del mismo modo, se permite el acceso justificado por representación (art. 18.2 LBAP); considerándose capacitados los representantes legales, en caso de un declarado incapaz, que los emancipados o jóvenes con 16 años cumplidos pueden acceder como si fueran mayores; y, por último, corresponde a los padres o representantes legales de los menores de edad poder acceder a la HC.

[379] Art. 15 "El médico informará al paciente de forma comprensible, con veracidad, ponderación y prudencia. Cuando la información incluya datos de gravedad o mal pronóstico se esforzará en transmitirla con delicadeza de manera que no perjudique al paciente".

[380] Art. 16. LBAP.

[381] Art. 18.3 LBAP.

[382] Se entiende por anotaciones subjetivas "las valoraciones personales, sustentadas o no en los datos clínicos de que se disponga en ese momento, que no formando parte de la historia clínica actual del/de la paciente o usuario/a, puedan influir en el diagnóstico y futuro tratamiento médico una vez constatadas".
Además "el personal sanitario deberá abstenerse de incluir comentarios o datos que no tengan relación con la asistencia sanitaria del paciente o que carezcan de valor sanitario": Art. 21 Decreto 29/2009, de 5 de febrero de Galicia, por el que se regula el uso y acceso a la historia clínica electrónica.

[383] AEPD, Resolución de 30 de marzo de 2007.

[384] AEPD, Resolución de 22 de noviembre de 2004.

compañías sanitarias tenían conocimiento de ello y, por tanto, sin posibilidad de oponerse a ello[385].

Dentro de este apartado de acceso por terceros, se incluyen los siguientes accesos a la HC: los realizados por las Administraciones Públicas sanitarias; el propio de la inspección sanitaria, debidamente acreditada; el realizado con fines judiciales, epidemiológicos, de salud pública, e investigación o de docencia; y el que pueden llevar a cabo Mutualidades y Compañías aseguradoras.

1. Acceso por las Administraciones Públicas sanitarias.

En el ámbito de la legislación sanitaria, se prevé el necesario intercambio de información en salud entre organismos, centros y servicios del SNS, permitiendo el acceso a la HC a los profesionales sanitarios que participan en la asistencia sanitaria "(…) *en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información (…)*"; todo ello, con la finalidad de la mejora de la atención sanitaria del paciente[386]. En este sentido, la LOPD se refería a la no necesidad de consentimiento del afectado cuando se tratara de datos tratados para el ejercicio de funciones propias de las Administraciones Públicas en el ejercicio de sus funciones[387].

En cuanto al acceso por personal con fines administrativos de gestión el acceso de este personal resulta imprescindible a fin de que la marcha del proceso asistencial del paciente no se vea paralizado; estando justificado en la medida que comprenda únicamente el acceso a los datos de la HC que se adecúen al cumplimiento de sus funciones, como establece el art. 16.4 LBAP, o que resulte "imprescindible para realizar las funciones que tiene encomendadas"[388]. No obstante, este precepto no contempla la necesidad de acceso de otro personal administrativo de los Servicios Regionales de Salud que realizan funciones que pueden considerarse accesorias, como los que prestan funciones en los

[385] Diario la Vanguardia, EFE Washington, 12-11-2019: https://www.lavanguardia.com/tecnologia/20191112/471545042307/google-datos-medicos.html.
[386] Art. 56 de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.
[387] Art. 6.2 LOPD
[388] Art. 13 Decreto 101/2005, de 22 de diciembre de la Junta de Castilla y León, por el que se regula la historia clínica.

ámbitos de la responsabilidad patrimonial o de la concesión de prestaciones complementarias. Por ello, deberán ser los propios centros sanitarios, los que establezcan distintos niveles de acceso a la HC considerando el tipo de funciones no asistenciales que realice este personal (citaciones, gestión del IVE, CSUR, etc.). En otro caso, estaríamos ante accesos indebidos o no autorizados.

El RGPD contempla dentro del concepto de tratamiento lo que denomina "comunicación por transmisión", que se correspondería con la comunicación-cesión de datos sanitarios entre Administraciones Públicas: organismos, centros y servicios del SNS, con la finalidad de recibir una mejor asistencia sanitaria[389].

Este intercambio de información entre Administraciones, que no requiere el consentimiento del titular de los datos, deberá adecuarse a la legislación vigente sobre protección de datos y a la LBAP[390]; la cual establece la obligación al Ministerio de Sanidad de facilitar la coordinación de las HC entre los distintos Servicios de Salud, estableciendo sistemas compatibles que hagan posible acceder por dichos servicios a la información de un mismo paciente "(…) *en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición*"[391].

Sin embargo, el RGPD para entenderla como lícita, habilita la comunicación de datos entre AAPP siempre que concurra alguna de las condiciones previstas en el art. 6.1, (a quien remite el propio art .8 LOPDGDD); siendo la primera, lógicamente, el consentimiento del afectado (*a*); y las restantes, a nuestros efectos, serían:

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

[389] La AEPD han mantenido un concepto amplio de cesión en el supuesto de que cedente y cesionario tengan la condición de AAPP.

[390] Ello es así en virtud de lo dispuesto en el art. 56 de la Ley 16/2003:
"Con el fin de que los ciudadanos reciban la mejor atención sanitaria posible en cualquier centro o servicio del Sistema Nacional de Salud, el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de salud individual, previamente acordados con las comunidades autónomas, para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione".

[391] Disp. Adic. 3ª de la LBAP.

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

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

Sin embargo, este planteamiento choca de plano con lo dispuesto en el art. 28.2 y 3 de LPAC[392], en el que contempla la comunicación de datos personales entre AAPP en el ámbito de la consulta de datos en ficheros o bases de datos, previstos para el ejercicio de sus propias funciones[393], con el consentimiento presunto del interesado; de forma que para la no realización de la comunicación de datos deberá constar la oposición expresa del interesado.

No obstante, sí parece que tendría encaje en alguna de las condiciones anteriores que califican el tratamiento como lícito, si se trata, dentro del ámbito administrativo público, de las transmisiones de datos entre AAPP, debiendo cada Administración permitir el acceso de otras Administraciones a los datos de los interesados que tengan en su poder, especificando "las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad"; estando disponibles únicamente para aquellos datos "que son requeridos a los interesados por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia, de acuerdo con la normativa reguladora de los mismos[394]. Aunque, en este supuesto habrá de tenerse en cuenta lo dispuesto en la Disp. Adic. 12ª RGPD, que establece la necesidad del consentimiento del interesado en los tratamientos del apdo.1 del art. 18 RGPD, exceptuando, entre otros supuestos, que existan razones de interés público importante del Estado. Por lo que, tratándose de cesiones de datos sanitarios entre Administraciones públicas para el ejercicio de sus funciones y funcionamiento del Sistema Nacional de Salud, supone un

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

[393] Como puede ser la solicitud de subvención por una persona dirigida a un Ministerio, en cuyo modelo de solicitud se contempla la posibilidad de consulta de datos necesarios para resolverla, siendo necesaria la consulta de datos fiscales mediante acceso a las bases de datos de la Agencia Tributaria; la cual se realizaría salvo si el interesado lo rechaza expresamente.

[394] Art. 155 1 y 2 de la Ley 40/2015, de 2 de octubre, de Régimen Jurídico del Sector Público.

interés público esencial definido en la Ley (Ley de Cohesión del Sistema Nacional de Salud), contemplando las garantías previstas en el apartado 9.2 g) RGPD y, por tanto, base jurídica suficiente para justificar el interés público de estos tratamientos de datos, sin exigirse el consentimiento del interesado.

2 Acceso por personal que ejerza funciones de inspección debidamente acreditado, estando obligado a guardar secreto.

Conforme al art. 16.5 LBAP "*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*".

3. Acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, e investigación o de docencia.

El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso[395]. En concreto, para el acceso con fines judiciales, epidemiológicos, de salud pública y de investigación o docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales y en la LGS, y demás normas de aplicación en cada caso. La LOPDGDD ha venido a modificar el régimen de tratamiento de datos de investigación en salud previsto en la LGS remitiendo a la normativa de protección de datos[396].

El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente (DNI, n.º de Seguridad Social, n.º de HC, etc.), separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato –datos anonimizados-, salvo que el propio paciente haya dado su

[395] SSAN de 8 de octubre de 2008 y 26 de noviembre de 2003.
[396] LOPDGDD, Disp.Adic.17ª.2.

consentimiento para no separarlos[397]. Esta disociación de datos deberá llevarla a cabo un profesional sanitario sujeto al secreto profesional o persona sujeta al mismo derecho o equivalente.

En el ámbito investigador, únicamente podrán utilizarse datos de la HC relacionados directamente con los fines de la investigación, sin que puedan revelarse hechos, características o circunstancias que permitan la identificación del paciente involucrado en el estudio de investigación.

Se contempla como excepción, la existencia de razones epidemiológicas o de protección de la salud pública, en la que las Administraciones sanitarias podrán acceder a los datos identificativos de los pacientes, cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población; además de las previstas en particular para biomedicina, en la Disp.Adic.17ª.2 de la LOPDGDD[398].

Así mismo, se exceptúan los supuestos de investigación de la autoridad judicial[399] en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente.

A fin de que una solicitud judicial genérica de la HC de un paciente no pueda atentar contra su intimidad, resulta imprescindible que dicha petición afecte a datos determinados y concretos de la HC, fundamentándose la necesidad de acceder a dichos datos[400]; lo que, de otra forma estaría quebrando el principio de proporcionalidad.

Quizás debería establecerse una especie de gradación de las solicitudes de acceso en función del tipo de proceso de que se trate. Así, tratándose de un proceso penal, en el que se ventila el interés público, tendría, en principio, más justificación realizar una menor

397 Art. 16.3 LBAP, modificada por la LOPDGDD.

398 A quien remite el propio art. 16.3 LBAP.

399 El art. 11.d) de la LOPD señalaba al respecto: "Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas".
Debe señalarse que los tribunales eclesiásticos, al no formar parte del Poder Judicial, quedan excluidos de esta excepción de solicitar el consentimiento del titular de los datos.

400 En este sentido se pronuncia el art. 17 del Decreto 101/2005, de 22 de diciembre de la Junta de Castilla y León.

discriminación del contenido de la solicitud del órgano judicial. En cambio, en el proceso civil, en el que pueden verse afectados terceras personas con intereses contrapuestos al del titular de los datos (p.ej. proceso de divorcio), esta discriminación parece absolutamente imprescindible a fin de proteger la intimidad del paciente.

Así, en el ámbito penal, como principio general hay que señalar como la confidencialidad de la HC cede ante la investigación de un delito penal; por cuanto el derecho a la intimidad, objetivo de la protección de la confidencialidad, cede ante un bien superior como pueden ser las actuaciones penales. En este sentido, la AP de Navarra entiende que incorporar al proceso la historia clínica completa de la denunciante constituiría:

> "(*…) una solicitud desproporcionada en relación con el fin pretendido de aportación de algún dato de interés en relación con los hechos objeto del procedimiento (…) En efecto, semejante solicitud alcanzaría a cuantos aspectos relativos a la salud de la denunciante hubieren sido objeto de algún tipo de consulta o tratamiento, resultando ser inaceptable la constancia de todo ello en este procedimiento, careciendo de justificación esa genérica e ilimitada pretensión de aportación de todos esos datos afectantes a su intimidad"*[401].

No obstante, la AEPD vino a determinar que, con carácter general, resulta necesario atender lo solicitado por el órgano judicial respecto del envío de datos de la HC de un paciente[402].

4. Otros accesos de la HC. Mutuas de Accidentes de Trabajo y Enfermedades profesionales

Las Mutuas son entidades colaboradoras con el régimen de gestión de las prestaciones de Seguridad Social, llevando a cabo el control y seguimiento de las prestaciones sanitarias de IT de los trabajadores de las empresas que gestionan; por ello, deben estar legitimadas

[401] Auto nº 463/2016, de 7 de diciembre de la Audiencia Provincial de Navarra, en el que se plantea recurso contra la denegación del Juzgado de Instrucción nº 4 de Pamplona del acceso completo a la historia clínica de un paciente.

[402] AEPD, Informe 36/2004, sobre cesión de datos de la historia clínica a órganos jurisdiccionales.

para que, a través de sus profesionales médicos, puedan acceder a las HC de los pacientes que gestionan con la finalidad de su asistencia sanitaria.

El acceso realizado por Compañías aseguradoras será objeto de estudio específico al tratar la problemática que afecta a determinadas cesiones de datos de salud (apartado 3).

v) Acceso a la Historia Clínica de personas fallecidas.

En el supuesto de personas fallecidas y sus datos sanitarios, nos encontramos con la necesidad de conjugar dos derechos que interactúan y que resultan necesario preservar a fin de evitar accesos injustificados por terceros: el derecho a la intimidad del paciente y el deber de secreto médico.

Como señala TRONCOSO REIGADA[403], el derecho a la protección de datos es un conjunto o instituto de garantía de otros derechos fundamentales, que, en ocasiones, como es el caso de la intimidad personal, no se extingue con la muerte; por lo que la HC de fallecidos "se encuentra amparada por la ley en la medida en que se refiere a personas físicas identificadas o identificables, que sólo dejará de estar tutelado si se disocia esta información".

La Exposición de Motivos de la LOPDGDD destaca la novedosa regulación (contenida en el art. 3)[404] de los datos referidos a las personas fallecidas, *"(…) pues, tras excluir del*

[403] TRONCOSO REIGADA, A., *La protección de datos sanitarios: La confidencialidad de la historia clínica, Protección de datos personales para servicios sanitarios públicos*, Agencia de Protección de Datos de la Comunidad de Madrid, 2008, p.30.

[404] "Artículo 3. Datos de las personas fallecidas.

1. Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

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.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido".

Sin embargo, el RGPD no es de aplicación a las personas fallecidas, por cuanto los datos de personas fallecidas en los que ya no hay personalidad jurídica no entran en su régimen, autorizando a que sean los propios Estados competentes a dictar la legislación correspondiente. Del mismo modo, la LOPDGDD lo excluye del ámbito de aplicación del Título I a IX, y de los artículos 89 a 42; de forma que esta materia se regirá por la legislación específica que resulte aplicable o supletoriamente por el RGPD y la LOPDGDD. No obstante, es posible el acceso a la HC del fallecido y, solicitar, en su caso, su rectificación o supresión en los siguientes supuestos:

a) los familiares o personas vinculadas al fallecido, siempre que no exista una prohibición legal o personal expresa del fallecido; la cual "no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante";

b) las personas o instituciones designadas expresamente para tal motivo y de acuerdo con las instrucciones indicadas;

c) si se trata de menores fallecidos y discapacitados, dichas facultadas se ejercerán por sus representantes legales o el Ministerio Fiscal, y en el caso de personas con discapacidad, además por la persona designada para ejercer sus funciones de apoyo.

Por su parte, la LBAP, limita el acceso de terceros a la HC de los fallecidos si afecta a su intimidad y a las anotaciones subjetivas de los profesionales, sin que, además, perjudique a derechos de terceros (art. 18.4).

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado".

2.3. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS DE SALUD

2.3.1. TRATAMIENTO DE DATOS DE PERSONALES

2.3.1.1. Consideraciones previas

Al referirnos al término protección de datos, debemos considerar, como ya hemos visto anteriormente, el art. 18.4 CE, de respuesta constitucional a la libertad informática como "una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", y la doctrina del TC contenida, entre otras, en las SSTC 94/1998[405] y 292/2000, en las que señala respectivamente que el derecho a la protección deberá garantizar al individuo el control y disposición sobre sus datos personales, en lo que refiere al uso y destino de modo de evitar el tráfico ilícito de estos, así como evitar que su uso resulten perjudiciales para la dignidad o el ejercicio de cualquiera de los demás derechos fundamentales conexos al de protección de datos personales. Por su parte, la STC 292/2000, hace referencia a este derecho como un derecho autónomo e independiente, que faculta al individuo a disponer y controlar que datos proporciona a un tercero, y qué tratamiento se dan a los mismos una vez obtenidos, permitiéndole tener acceso a sus datos y oponerse en cualquier momento al uso y posesión de los mismos por parte de terceros.

Con la entrada en vigor del RGPD se ha procedido a abordar con mayor rigor la protección de datos por el conjunto del Ordenamiento europeo y, en la medida en que el derecho a la protección de datos no es absoluto, el tratamiento de datos supone considerar el derecho a la protección de datos en relación con otros derechos fundamentales que han de ser respetados, debiéndose proceder a conciliar los derechos en juego, aplicando de forma equilibrada los derechos afectados, conforme al principio de proporcionalidad (Considerando 4). En este sentido, el Considerando 153 RGPD se refiere a la necesidad de que el derecho a la protección de datos de los Estados miembros debe conciliar "(…) *con las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria*…"; y, en todo caso, el tratamiento de datos personales debe respetar las libertades y derechos fundamentales, en la medida de que no estamos ante un derecho absoluto.

[405] Que considera el derecho a la protección de datos como la facultad que tiene el interesado para oponerse al uso o a determinado uso de los mismos, ya fuere porque sean utilizados con un fin distinto al cual fueron recabados o porque el uso de los mismos, puedan ser considerados incorrectos o lesivos de su intimidad.

El RGPD se refiere al tratamiento considerando un contenido amplio del mismo: *"(...) 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*"[406]. Por tanto, queda claro que, al referirnos al tratamiento de datos, nos referimos a cualquier manejo que se ejecute sobre los datos de una persona, independientemente del modo que se realice, por lo que quedan incluidos los medios manuales, mecánicos e informatizados.

Al mismo tiempo, ha de considerarse la posible existencia de excepciones a la prohibición general de tratamiento de determinadas categorías de datos especiales justificada en base al interés público[407], según lo determinado en el Derecho nacional o europeo, y "(…) *siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales* (…)". De esta forma, el nuevo régimen de protección y tratamiento de datos acuñado por el nuevo Reglamento otorga especial interés a aspectos no sólo técnicos y jurídicos, sino culturales, sociales o económicos.

En la sentencia del STC 76/2019[408], relativa a las opiniones públicas de las personas, se expone el actual régimen jurídico del tratamiento de datos personales, aludiendo al contenido, tanto del RGPD, como de la LOPDGDD, al señalar que, de acuerdo con el apartado 1 del art. 9 RGPD, dirigido al "tratamiento de categorías especiales de datos"; resulta prohibido el tratamiento de datos personales relativos a la salud, así como los datos que revelen las opiniones políticas, el origen étnico o racial, las convicciones religiosas o filosóficas o la afiliación sindical, el tratamiento de datos genéticos y los datos biométricos dirigidos a identificar de manera unívoca a una persona física, o a su orientación sexual. No obstante, el apartado 2 del mismo precepto autoriza el tratamiento

[406] Art. 2 RGPD.

[407] En base a razones diversas, como seguridad, investigación de infracciones y delitos, salud pública, legislación laboral, aspectos sociales, como pensiones, etc. Como resulta de los Considerandos 52,54,55 y 56.

[408] STC 76/2019, de 22 de mayo, estima el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra el apartado 1 del art. 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado a esta por la disposición final tercera, apartado dos, de la LOPDGDD, declarándolo inconstitucional y nulo por considerar que la autorización a los partidos políticos a recopilar datos relativos a las opiniones políticas de las personas vulnera los art. 18.4 y 53.1 de la CE.

de este tipo de datos cuando concurra alguna de las diez circunstancias allí previstas [letras a) a j)].

2.3.1.2. Licitud del tratamiento

Todo tratamiento de datos personales debe ser lícito, para lo que se exige el consentimiento del interesado o tratarse de supuestos previstos legalmente. Así el art. 6 del RGPD establece las condiciones para que el tratamiento sea lícito de forma general, que luego la LOGDPDD en su Título IV se encarga de establecer de forma no exhaustiva para cada tipo particular de tratamiento; en concreto, para los datos de salud, se contiene la regulación en la Disp. Adic.17ª, como veremos seguidamente al tratar el apartado relativo a "otras bases legitimadoras (distintas del consentimiento del titular) del tratamiento de datos de salud".

El hecho de que se considere lícito no libera a los responsables de adoptar las medidas de responsabilidad activa establecidas tanto en el Reglamento como en la ley. Además, el tratamiento debe ser leal, de forma que para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

El tratamiento de datos personales para ser calificado como lícito o legítimo debe adecuarse al principio de calidad de los datos[409], que exige que los datos recabados han de ser "adecuados, exactos pertinentes, actualizados y no excesivos… teniendo en cuenta los fines para los que se recogieron o trataron; por tanto, sólo será posible recabar aquellos datos que sean estrictamente necesarios para la finalidad que justifica su obtención[410].

[409] Contenido en el art. 94.2 de la LOPDGDD indirectamente al tratar el derecho al olvido.

[410] Como señala GIL MEMBRADO, C., *La historia clínica. Deberes del responsable del tratamiento y derechos del paciente*, Comar, 2010, cap.I, normativa, pp. 1146-1147; habría que considerar ilícita o ilegitima la inclusión en la HC de datos sobre la orientación ideológica del paciente, sin ninguna relación con la finalidad asistencial de la misma. Sin embargo, ello no impide que otros datos de contenido no sanitario figuren en la HC, pero siempre con un alcance restringido y que tengan importancia para la asistencia sanitaria del paciente.

2.3.1.3. Responsable-Encargado de tratamiento

El tratamiento de los datos personales como hemos visto podrá pasar por sucesivas etapas y teniendo acceso a los mismos distintas empresas u organizaciones; por tanto, es necesario determinar quiénes pueden efectuar el tratamiento de estos datos, para ello, se han establecido dos figuras principales para gestionar el tratamiento de datos personales: por un lado el responsable del tratamiento de los datos que es quien decide la forma y finalidad con que se tratan los datos y por otro, el encargado del tratamiento de los datos, que será quien conserve y trate los datos por cuenta del responsable[411]. Como señala NUÑEZ GARCÍA, en base a lo dictado por el GT29[412], se trata de una ficción jurídica, ideada inicialmente por la Directiva 95/46, basada en que estamos ante un tratamiento efectuado por delegación, en el que el encargado, como prestador de servicios, está obligado a seguir las instrucciones del responsable, con la consecuencia de que el acceso concedido no es considerado protección de datos[413].

En virtud de esta ficción jurídica, los datos no son revelados a un tercero, sino que permanecen en la esfera de control del responsable, no obstante, sean gestionados por una entidad distinta de las dos figuras (tercera entidad)[414]. Por tanto, como señala ALMUZARA ALMAIDA, el encargado no tiene capacidad para determinar los fines y los medios del tratamiento, ya que estos no se transmiten desde la posición del responsable, siguiendo dentro su órbita de control[415].

Así, el RGPD (art. 4.8) define el encargado del tratamiento como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento";* de ahí, que no tenga poder de decisión sobre el tratamiento de datos personales, que permanece en el responsable tratamiento.

411 Para más información sobre la figura del responsable del tratamiento, ver LESMES SERRANO, *op.cit.*, pp. 115-11.

412 GT 29, Dictamen 1/2010, sobre los conceptos de "responsable del tratamiento y encargado del tratamiento", p.28. Disponible en: http//ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.-

413 NUÑEZ GARCÍA, J.A., "El encargado del tratamiento", en *Reglamento General de protección de datos*…, *op.cit.*, pp. 321-323

414 PIÑAR MAÑAS, J.L., "Novedades en relación con la figura del encargado del tratamiento", en ZABÍA DE LA MATA, J., (Coord.), *Protección de Datos: Comentarios al Reglamento, op.cit.,* p.219.

415 ALMUZARA ALMAIDA, C., "El encargado del tratamiento, en *Reglamento General de protección de datos*…, *op.cit.*, p. 324.

En este sentido, el GT 29, ha señalado como requisitos para considerarse estar ante un encargado del tratamiento: "*por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste;* pudiendo, el responsable del tratamiento" *decidir delegar todas o una parte de las actividades de tratamiento en una organización externa, es decir —como se señala en la exposición de motivos de la propuesta modificada de la Comisión—, en "una persona jurídicamente distinta que actúa por su cuenta"*[416].

Aunque lo normal es que se trate de una persona física o jurídica distinta a la organización propia del responsable del tratamiento, puede suceder que una organización o empresa puede aglutinar las dos figuras de responsable y encargado del tratamiento*: "un mismo ente puede actuar a la vez como responsable del tratamiento para determinadas operaciones de tratamiento y como encargado del tratamiento para otras, y la condición de responsable o encargado debe evaluarse respecto de unos conjuntos muy determinados de datos u operaciones"*[417].

Y en relación con esta última cuestión, lo que resalta el GT29 es que el responsable del tratamiento puede decidir *delegar todas o una parte de las actividades de tratamiento en una organización externa, es decir —como se señala en la exposición de motivos de la propuesta modificada de la Comisión—, en «una persona jurídicamente distinta que actúa por su cuenta».*

En este sentido, el Grupo de Trabajo del Artículo 29 (GT29), señaló en su Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", WP 169, adoptado el 16 de febrero de 2010, que para estar ante un encargado del tratamiento *tienen que darse dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste.* Y en relación con esta última cuestión, lo que resalta el GT29 es que el responsable del tratamiento puede decidir *delegar todas o una parte de las actividades de tratamiento en una organización externa, es decir —como se señala en la exposición de motivos de la propuesta*

[416] GT 29 Dictamen 1/2010, de 16 de febrero.
[417] *Ibid.*

modificada de la Comisión—, en «una persona jurídicamente distinta que actúa por su cuenta».

Cuando el tratamiento de datos es realizado para otra empresa, el responsable del tratamiento de los datos solamente podrá acudir a un encargado que ofrezca garantías suficientes. Estas, deberán estar incluidas y claramente establecidas en un contrato que requerirá firmarse por escrito por todas las partes implicadas en el tratamiento de los datos. El contrato también deberá contener una serie de cláusulas obligatorias, como por ejemplo que el encargado del tratamiento solamente tratará datos personales por encargo del responsable del tratamiento de los datos[418].

Para la elección del encargado del tratamiento, el responsable del mismo debe seleccionar a quien le ofrezca garantías suficientes (a través de la adhesión a códigos de conducta o un certificado de protección de datos) en la implantación y mantenimiento de medidas técnicas y organizativas adecuadas, incluyendo la seguridad del tratamiento (conforme al RGPD, art. 32), y que al mismo tiempo pueda garantizar los derechos de las personas afectadas; para ello, deberá disponer de los conocimientos necesarios y recursos precisos, conforme al Considerando 81 del Reglamento.

En el supuesto de que el tratamiento de los datos implique una transferencia de datos fuera de la Unión Europea, se deberá velar por el fiel cumplimento de los requisitos exigidos en el marco del Reglamento, asegurando que el tratamiento de los datos cumpla con las medidas adecuadas para garantizar el ejercicio de los derechos asociados al tratamiento de los datos personales, y teniendo en cuenta las siguientes consideraciones[419]:

a) bien que el país u organismo receptor de los datos cuente con una decisión de adecuación de la Comisión Europea;

b) bien que el receptor haya tomado las medidas necesarias para salvaguardar los derechos de los implicados, como puede ser, por ejemplo, la inclusión de cláusulas específicas en

[418] Vide documento conjunto de la AEPD, Autoridad Catalana de Protección de Datos y Agencia Vasca de Protección de Datos, "Guía para la elaboración de contratos entre el responsable y el encargado del tratamiento", 16 de mayo de 2018.
[419] Art. 5.2 RGPD.

el contrato celebrado entre el exportador e importador no perteneciente a la Unión Europea;

c) que la transferencia esté basada en las excepciones establecidas, como lo es el consentimiento del interesado después de haber sido informado inequívocamente sobre los riesgos que implica la transferencia a un país u organización que no cuenta con las garantías suficientes.

El tratamiento de datos por el encargado se regirá por un contrato entre el responsable y el encargado del tratamiento, en el que se plasmarán los derechos y obligaciones de ambos, conforme a lo previsto en el apartado 3 del art. 28; debiendo figurar, entre otras, las siguientes cuestiones:

a) Tratará los datos personales siguiendo únicamente las instrucciones del responsable del tratamiento.

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" (b).

d) "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".

h) "Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo".

Otras obligaciones serían:

- Cooperar con la autoridad de control, facilitando la información que ésta solicite y dando cumplimiento a lo ordenado (art. 31 RGPD).

- Implantación de medidas de seguridad del tratamiento, aplicando medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (art. 32 RGPD).

Por último, está sujeto al régimen sancionador previsto en los arts.83 y 84 RGPD (que distingue si se trata o no de una empresa como encargada del tratamiento), concretado en las disposiciones del Título IX de la LOPDGDD, para los supuestos de incumplimiento o infracción de la normativa sobre protección de datos.

Corresponsable del tratamiento

Cabe la posibilidad (prevista en el art. 26 RGPD) que pueda existir un tratamiento conjunto de datos personales entre dos o más responsables del tratamiento, si estos "determinan conjuntamente los objetivos (finalidad) y establecen los medios (para realizarlos) del tratamiento necesarios para el mismo.

Sobre esta figura, el Supervisor de Datos de la Unión Europea (SUEPD) se ha pronunciado en similares términos a los de la Opinión 1/2010 del GT 29, aunque viene a realizar alguna diferenciación, sobre la base de la última jurisprudencia del TJUE; diferenciando entre la corresponsabilidad aplicada a todo el proceso de tratamiento de los datos, de la corresponsabilidad aplicada a alguna fase del mismo; de forma que a las otras fases se aplicaría una responsabilidad separada. Además, en línea con la STJUE *Jehovan*[420], si uno de los corresponsables no trata datos en ningún momento será corresponsable si ha decidido conjuntamente los fines y los medios del tratamiento[421].

Trasladándonos al ámbito sanitario, el responsable del tratamiento de datos que, forma parte de la historia clínica, es el médico o el centro sanitario, público o privado. La asistencia a una consulta médica, bien directamente o a través de un centro sanitario público o privado, solicitando asistencia sanitaria lleva implícita la no necesidad de consentimiento del paciente para tratar sus datos personales; aunque deberá ser informado de que tiene derecho a solicitar el acceso a sus datos personales al responsable del tratamiento, así como de rectificación (tratándose de datos sanitarios corresponde al médico decidirla) o supresión, limitación de tratamiento, oposición, o a ejercer el derecho

[420] STJUE C-25/17, *Jehovan todistajat*, de 10 de julio de 2018.

[421] SEPD "*Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725"*, 7.11.2019.

a la portabilidad de los datos; pudiendo, estos derechos, sufrir limitaciones por razones de interés público conectado con la salud o por el cumplimiento de obligaciones legales.

Para el acceso (tanto electrónico como en papel) del paciente de su HC deberá dirigirse al responsable del tratamiento, considerando las particularidades previstas en la LBAP, como que no puede ejercitarse en perjuicio del derecho de terceros a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas. El acceso a la HC, además del propio paciente, puede realizarse por el responsable y el encargado del tratamiento (actúa por cuenta del responsable), como las empresas prestadoras de servicios externos sanitarios (clínicas o centros de pruebas diagnósticos o analíticas), cuyas obligaciones vendrán delimitadas en un contrato y que deben velar por la seguridad de los datos por parte de las personas dependientes de ellas que traten datos de pacientes. Tanto el responsable como el encargado del tratamiento (definidos en el art. 4 RGPD) estarán sujetos al deber de confidencialidad, secreto médico (en su caso), art. 5 LGDPDD.

Además, el paciente tendrá derecho a conocer del responsable del tratamiento si sus datos están siendo tratados o no; si lo estuvieran, podrá acceder a ellos y, además, deberá serle comunicada la información definida en el art. 15 RGPD.

En el apartado correspondiente a la seguridad de los datos sanitarios, se ha hecho referencia a la responsabilidad proactiva por parte del responsable en el tratamiento de datos de salud, que deberá aplicar … "medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento (art. 24.1), desde el diseño y por defecto, como la seudonimización y la minimización de datos (art. 25).

2.3.2. CONSENTIMIENTO Y OTRAS BASES LEGITIMADORAS DEL TRATAMIENTO DE DATOS DE SALUD

El consentimiento constituye uno de los requisitos fundamentales de la protección de datos exigido para garantizar un adecuado tratamiento de los datos personales del interesado, y que, en la medida en que el titular es el dueño de los datos, sólo con su

autorización es posible tratar esos datos, busca un mayor control sobre la recogida y el tratamiento de los datos personales.

Puede decirse que "El consentimiento es la llave de todo el tratamiento de datos personales". Salvo las excepciones legalmente previstas, el consentimiento da acceso al tratamiento de nuestros datos personales, lo legitima y permite hablar de un control (total, en la medida en que puede retirarse el consentimiento prestado) de los mismos; esto es, haber sido conscientes o no de que nuestros datos están siendo tratados"[422]. Al mismo tiempo, supone el principal mecanismo de exteriorización de la voluntad del titular de los datos[423]; no siendo suficiente el reconocimiento del derecho a ser informado para satisfacer la pretensión del control sobre la información.

Frente a la normativa inicial sobre la materia, en la que el interesado no llegaba a tener un control pleno de la totalidad de sus datos personales con la entrada en vigor del RGPD, la situación se ha modificado al otorgar al interesado el máximo poder de disposición y control sobre sus datos personales, a través de la manifestación del consentimiento (o su retirada) y del ejercicio de los derechos al acceso, rectificación, supresión, olvido y portabilidad.

2.3.2.1. Requisitos del consentimiento

Este apartado pretende analizar cuáles son los requisitos que debe cumplir el consentimiento para constituir el mecanismo de contralor del tratamiento de los datos por parte de su titular. El consentimiento constituye la regla general pues es necesaria su concurrencia para el tratamiento y cesión de los datos del individuo, según establecen los artículos 6.1. a) y 9.2.a) del RGPD.

Así, el primer supuesto que legitima el tratamiento de datos de salud es que el interesado haya prestado "su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados…" (art. 9.2.a) RGPD). Vemos, que la diferencia con el consentimiento como criterio de licitud de tratamiento de las categorías generales

[422] ARENAS RAMIRO, M., *Reforzando el ejercicio del derecho a la protección de datos personales, hacia nuevo derecho europeo de protección de datos*, Tirant Lo Blanch, Valencia, 2015. p.329.
[423] VIZCAÍNO CALDERON, M., *Comentarios a la Ley Orgánica de Protección de Datos*, Civitas, Madrid, 2001, p. 84.

de datos personales -previstas en el art. 6.1.a) es precisamente que se exige, además, que el consentimiento sea explícito (también se exigía en la Directiva 95/46 CE, art. 8.2.a) en la categoría de datos especiales).

Sin embargo, hay que señalar que la exigencia del consentimiento explícito como base legitimadora del tratamiento de categorías especiales de datos personales no tiene un carácter absoluto, por cuanto el propio art. 9.2.a) *in fine* contiene la excepción de que "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". De ahí, que tanto el Derecho de la UE como de los Estados miembros puedan establecer otras condiciones para la licitud del consentimiento, añadidas al consentimiento explícito del interesado; de forma que este no sirva o no sea suficiente para considerar lícito el tratamiento de categorías especiales de datos. A ello, se refiere la propia LOPDGDD al señalar que "a fin de evitar situaciones discriminatorias, 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" (art. 9.1). No obstante, sigue señalando la ley que "lo dispuesto en el párrafo anterior 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".

De esta forma, el consentimiento explícito será base suficiente para legitimar el tratamiento de datos de salud, datos genéticos y datos biométricos.

Se desprende de las definiciones legales comentadas que en ellas se encuentran insertos los requisitos que tal autorización debe cumplir para que sea considerada como efectiva, como válida, esto es, la voluntad libre, específica, informada e inequívoca[424].

La AEPD se refirió a dichos requisitos que debe cumplir el consentimiento como:

"a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil. b) Específico, es decir referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como

[424] En este apartado se han considerado las Directrices del GT29 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 adoptadas el 28 de noviembre de 2017 revisadas por última vez y adoptadas el 10 de abril de 2018.

impone el artículo 4.2 de la Ley Orgánica 15/1999. c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce.

Precisamente por ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen. d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento[425].

Al tratarse de un asunto de tanta complejidad como es el tratamiento de datos personales y los derechos fundamentales que pudieran llegar a ser vulnerados por su mal uso, el legislador europeo, buscó garantizar que el titular de los datos conozca realmente que es lo que está autorizando al expresar su consentimiento. Es por ello, que establece que el consentimiento deberá ser expresado libremente y de modo inequívoco. Y es considerado de tal importancia, que además es preciso que el interesado sea informado sobre la finalidad y tratamiento posterior de sus datos.

Asimismo, es necesario que el mismo haya sido dado de forma específica e inequívoca mediante un documento expresado en un lenguaje claro y preciso. El consentimiento, por tanto, deberá ser una declaración o una acción afirmativa, excluyendo el consentimiento tácito como forma lícita de consentir el tratamiento de datos, considerándose que esta novedad supone una mayor garantía o control al afectado sobre sus propios datos[426]. Por tanto, el consentimiento debe ser expreso, no cabe el consentimiento tácito o el deducible del silencio, como se permitía en la anterior legislación sobre protección de datos, suprimiéndose así la alterativa anterior de las casillas previamente señaladas.

Tanto si el consentimiento adopta la forma de declaración escrita, utilizando medios manuales o electrónicos, además de poder marcarse una casilla o seleccionarse una opción determinada, como si se emite verbalmente, deberá poderse deducir de una forma clara la aceptación por el interesado del tratamiento de sus datos personales.

[425] AEPD, Memoria del año 2000, https://www.aepd.es/media/memorias/memoria-AEPD-2000.pdf.

[426] MARTÍNEZ-ROJAS, A., "Principales aspectos del consentimiento en el Reglamento general de protección de datos de la Unión Europea", en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 42, septiembre-diciembre 2016, p. 73.

La manifestación de voluntad ha de ser libre, inequívoca, específica e informada. El consentimiento ha de estar prestado en libertad, sin que el afectado esté sometido por ningún tipo de presión, engaño o manipulación, o como señala el Reglamento, no puede ser un fundamento jurídico válido cuando haya un desequilibrio claro entre el interesado y el responsable del tratamiento (Considerando 43), citando dos ejemplos al respecto: cuando no se puedan autorizar separadamente las distintas operaciones de tratamiento de datos personales, aunque fuera adecuado en el caso de que se trate; y cuando el cumplimiento de un contrato, incluida la prestación de un servicio, dependa del consentimiento, aun cuando éste no sea necesario para dicho cumplimiento.

Respecto del requisito de la libertad del consentimiento, no está en duda el poder de elección del interesado, quien tiene en todo momento la libertad para consentir. Sin embargo, la falta de información sobre el tratamiento de sus datos, la finalidad del mismo y toda la información que sobre este proceso se requiera obtener, son necesarias para poder consentir de forma libre[427].

La libertad de la voluntad de autorizar el consentimiento conlleva un contrapeso y es la libertad para revocarlo. Se entiende por revocación la acción del titular de los datos de dejar sin validez o efecto el consentimiento prestado previamente[428]. El ejercicio de este derecho debe hacerse de conformidad con lo establecido en la LOPDGDD, que remite a su vez al RGPD, que expresa que el interesado tendrá derecho a retirar su consentimiento en cualquier momento, sin más limitaciones que dicha manifestación, incluso se establece como principio que será tan fácil retirar el consentimiento como darlo[429].

Así, el libre ejercicio del consentimiento debe entenderse que no puede estar sometido a ningún tipo de coacción o intimidación que lleve a alterar el sentido de la voluntad de dicha persona[430]. Ello implica que cuando se utiliza otro tipo de coacción como la fuerza, la intimidación o el miedo para obtener la aprobación del interesado, se estaría

[427] En varios dictámenes, el GT29 ha estudiado los límites del consentimiento en situaciones en las que este no puede darse libremente. Es el caso, en particular, del Dictamen 15/2011 sobre la definición de consentimiento (WP 187) y el Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos.

[428] MESSIA DE LA CERDA BALLESTEROS, J.A., *La Cesión o Comunicación de Datos de Carácter Personal*, Thomson-Civitas, Madrid, 2003, p. 252.

[429] Art. 7.3. RGPD.

[430] ARENAS RAMIRO, M., *El Principio del Consentimiento en los Estados miembros de la Unión Europea*, Tirant lo Blanch, Vol.2, Valencia, 2007, p. 170.

invalidando el consentimiento puesto que se estaría en presencia de un supuesto de violencia negatorio de la libre voluntad.

La jurisprudencia se ha pronunciado respecto de la intimidación obligando a ciertos requisitos para que se invalide el consentimiento; por ejemplo, que la violencia que se ejerza sobre el interesado provenga de acto injusto o que la intimidación provenga también de una injusta e ilícita amenaza, tan contundente que el interesado se obligue a que su voluntad se convierta en contraria a sus intereses[431]. Además, la manifestación de voluntad ha de ser inequívoca, lo que implica que no exista ninguna duda de que el afectado quiere prestar el consentimiento. Por tanto, el consentimiento no se puede deducir de los actos del afectado, sino que necesaria una acción u omisión concreta por la que se concluya que existe consentimiento[432]. Así, Los tribunales han expresado que el consentimiento será inequívoco cuando sea incuestionable[433].

Al mismo tiempo, el consentimiento ha de ser específico, en el sentido de que el consentimiento que preste el afectado se refiera exclusivamente a una situación concreta y perfectamente determinada, excluyendo los consentimientos genéricos[434]. No es que no se pueda otorgar el consentimiento para varios tratamientos con objetos o finalidades distintas, si no que de ser necesario el consentimiento en esos términos, será obligatorio que dicho consentimiento se exprese claramente para todas ellas o para cada una de ellas individualmente.

Por tanto, la manifestación de voluntad debe ser específica; lo que implica que debe ser concreta para un tratamiento concreto y estar referida a todas las actividades incluidas en el tratamiento para el que se presta el consentimiento; ya que el consentimiento debe referirse además de aquello que afecta al tratamiento a la finalidad para la que se obtienen los datos, por lo que el afectado debe conocer de las actividades que componen el

[431] AP de Sevilla, de 20 de junio de 2006, FJ 2.

[432] SSAN de 28 de octubre de 2016 y 15 de julio de 2016, entre otras: "El principio de consentimiento expresado conllevará, por tanto, la necesidad del consentimiento inequívoco del afectado para que puedan tratarse sus datos de carácter personal, permitiéndose así a aquel ejercer efectivo el control sobre dichos actos y garantizando su poder de disposición sobre los mismos. Dicho consentimiento deberá prestarse de forma expresa, oral o escrita, o de manera tácita, mediante actos reiterados y concluyentes que revelen su existencia. Ahora bien, tal y como ha expresado esta Sala reiteradamente, el consentimiento ha de ser necesariamente "inequívoco. De modo que ha de aparecer como evidente, o lo que es lo mismo, que no admita duda o equivocación, pues éste y no otro es el significado del adjetivo utilizar para calificar el consentimiento".

[433] SAN de 9 de mayo de 2007.

[434] SAN de 24 de marzo de 2006.

tratamiento; es decir, que debe estar informado. Así, el consentimiento ha de estar precedido de una información previa, comprensible suficiente, precisa, inequívoca y ofrecida en el momento adecuado.

Esta información, trasladada al ámbito sanitario, es susceptible de diferenciarse: por una parte, la necesaria para proceder al tratamiento de los datos de salud, y de otra, la información de carácter clínico o asistencia que se proporciona al paciente y, que como veíamos, constituye el presupuesto del consentimiento posterior del afectado, y que a diferencia de la primera resulta necesaria cada vez que se produce un acto médico.

La LOPDGDD y el RGPD lo configuran de distinta forma. Así, para la LOPDGDD, "*Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas"*[435]. Por su parte, el RGPD, establece: "*Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento*"[436].

Por su parte, la jurisprudencia lo ha expresado muy bien en el sentido de que el consentimiento debe ser explícito, dado para una situación particular de la que se conocen todos los aspectos: la autorización debe ser específica cuando el interesado que lo otorga lo hace sobre sobre un objeto concreto[437].

Además, el consentimiento ha de ser eficaz. Así, no lo será en el caso de que se hubiera dado la autorización sin el conocimiento pleno de lo que se estaba autorizando; bien por propia incapacidad física o psíquica de la persona o porque la propia información haya sido deficiente, inexacta o incompleta, o suministrada de forma inentendible, en cuyo caso estaríamos ante una vulneración del consentimiento informado, y por tanto viciado de nulidad. Igualmente será ineficaz cuando exista un exceso del ámbito de la autorización concedida, o como expresa el TC, cuando se "(…) *subviertan los términos*

[435] Art. 6.2. LOPDGDD.
[436] Art. 7.3. RGPD.
[437] SAN de 17 de abril de 2007, FJ 7.

y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida (…)[438].

2.3.2.1.1. Especificidades del consentimiento para el tratamiento de los datos de salud

En el apartado del tratamiento específico de datos de salud, como ya comentamos al hablar de la HC, el choque legislativo que supone la aplicación del principio de consentimiento expreso requerido por la normativa de protección de datos y la aplicación de la normativa sanitaria, que prevé el consentimiento verbal como principio básico en la asistencia sanitaria (LBAP).

Así, el consentimiento informado implica "la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a la salud" (art. 8.3. LBAP). De forma que el paciente, después de recibir la información prevista en el art. 4 LBAP (como mínimo la que comprenda la finalidad y naturaleza de la intervención, sus riesgos y consecuencias), y después de "haber valorado las opciones propias del caso", con especial necesidad de información sobre los riesgos de la intervención sanitaria (art. 8.3), procederá a emitir o no su consentimiento por escrito.

Por ello, salvo para los casos (consentimiento escrito) de "intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente" (art. 8. 2), la regla general es la emisión del consentimiento verbal, que choca con la regla general del consentimiento expreso en la normativa general sobre protección de datos y, que está plenamente justificada en la medida en que, de otra forma, se podría producir una burocratización sanitaria en perjuicio de la propia asistencia sanitaria. A ello, habría que añadir las situaciones de

[438] STC 196/2004, FJ 2, citada por la STC 159/2009, FJ 3.

urgencia en las que por la propia situación (de inmediatez) o por la imposibilidad de prestar el consentimiento el paciente (ni sus familiares) no puede recabarse éste.

Además, la trascendencia de que la información previa al acto médico sea prestada adecuadamente justifica que una información inexistente, insuficiente, o no transmitida de forma adecuada a las características del paciente, determinan la exigencia de responsabilidad por infracción de la *lex artis ad hoc.*

Sobre el carácter de consentimiento verbal como regla general en el ámbito sanitario (distinto del consentimiento expreso exigido por la normativa sobre protección de datos), la justificación la encontramos en la propia esencia de la actividad sanitaria, como actuación prioritaria básica, que persigue, ante todo, la curación o protección de la salud; de forma que para una gran parte de actuaciones médico-sanitarias el paciente emite de forma verbal el consentimiento, que de exigirse su formalización escrita podría atentar contra la necesaria agilidad que debe tener la prestación de la asistencia sanitaria, en proporción al grado de necesidad de atención del paciente.

La exigencia de consentimiento escrito para las actuaciones médico-sanitarias que, en general entrañen más riesgo para el paciente, tiene su justificación en la consideración de su carácter esencial previo a cualquier actuación médico-sanitaria; por cuanto el derecho constitucional a la integridad física (art. 15 CE) exige que cualquier actuación sobre el cuerpo humano deba estar precedida de una conformidad del propio sujeto, a quien corresponde decidir sobre si acepta o no que médicamente se intervenga sobre su propio cuerpo. De forma que, de no darse esa conformidad o consentimiento o estar este viciado por ser incompleto o inadecuado estaríamos ante un acto médico sujeto a responsabilidad. De ahí, el que, como degeneración de la llamada "medicina defensiva", para los profesionales médicos el formalizar correctamente el consentimiento del paciente constituya el elemento esencial para poder valorar su correcta actuación profesional en el caso de una acción judicial o administrativa de responsabilidad.

Además, en algunos casos puede entenderse prestado el consentimiento. Así, se permite al personal médico y a las autoridades sanitarias el acceso a la información médica de carácter personal derivada de las medidas de vigilancia y control de la salud de los trabajadores, por lo que pueden acceder a los datos personales del interesado sin su

consentimiento[439]. No obstante, la AEPD limita dicho acceso, siempre y cuando se hubiera informado previamente al trabajador conforme a la normativa de protección de datos.

2.3.2.1.2. En cuanto a la forma de prestar el consentimiento

Por otra parte, la forma de expresar el consentimiento es de suma importancia desde el punto de vista de lo exigido por el legislador, el cual puede obtenerse, siendo expreso tal como lo indica la normativa vigente, mediante cualquier medio en el que el interesado pueda dejar prueba de la manifestación de su voluntad, en ese sentido, los instrumentos más comunes son los escritos.

El medio escrito (y, en mayor grado, si incluye la firma del titular) es el más adecuado y garantista de dejar constancia de forma expresa de la autorización del consentimiento y, por tanto, de acreditar que el mismo ha sido prestado. Dejamos a salvo, como hemos señalado, la excepción que supone que la actuación sanitaria que no requiera de intervenciones y pruebas diagnósticas que entrañen riesgo al paciente se lleve a cabo con el consentimiento verbal del afectado.

Cuando se requiere el consentimiento por medios electrónico o por internet, deberá recabarse de "(…) *tal forma que resulte imposible la introducción de dato alguno sin que previamente el afectado haya conocido la advertencia que contenga las menciones a las que nos hemos referido, pudiendo servir como prueba del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho referencia. Todo ello tiene por objeto asegurar que el consentimiento de los afectados sea efectivamente específico e inequívoco tal y como exige la Ley*"[440].

Por su parte las Directrices del GT29 reconocen como medio de prueba la conservación del llamado "*worflow*" o flujo de datos, dentro de los cuales se encuentra la dirección IP

[439] Art. 22.4. de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
[440] AEPD, Informe 0049/2007. Disponible en: https://www.aepd.es/informes/historicos/2007-0049.pdf.

del interesado, el sistema operativo, la versión del navegador, los cuales constituyen en su conjunto la huella digital[441].

2.3.2.2. Condicionantes de la licitud del consentimiento

Para que el consentimiento sea considerado lícito, además, deberá reunir ciertas condiciones formales y sustanciales que se encuentran reguladas en el artículo 7 del RGPD, las cuales desarrollaremos siguiendo el orden establecido por el artículo.

1. "*Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales*".

El considerando 42, establece un supuesto excepcional al exigir al responsable del tratamiento que entregue al interesado un modelo de declaración de consentimiento a fin de garantizar que es consciente sobre el consentimiento prestado y su alcance; el cual deberá contener " (…) *una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas*".

Queda claro que la obligación del responsable del tratamiento excede de la acreditación del consentimiento, ya que, además, deberá demostrar que el interesado ha expresado el consentimiento de forma libre, con conocimiento claro sobre la extensión, finalidad y consecuencia de la autorización que otorga y los riesgos que conlleva, y deberá demostrar también que el interesado ha comprendido las condiciones mencionadas sin que existan condicionamientos que pudieran interferir en la decisión tomada por el interesado.

2. "*Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil*

[441] Directrices del GT29 sobre el consentimiento en el sentido del RGPD, adoptadas el 28 de noviembre de 2017.

acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento".

Esta exigencia del RGPD tiene importancia en el ámbito sanitario, en el que se impone la distinción entre lo que constituye el consentimiento (informado) previo a la realización del acto médico y vinculado a la autonomía del paciente, del caso del consentimiento como presupuesto de licitud del tratamiento de datos personales en el contexto de la asistencia sanitaria o de la investigación biomédica.

Con relación a este apartado, debemos atender la cantidad de exigencias que incluye. En principio el consentimiento deberá establecerse del mismo modo que el resto de los asuntos, pero de una manera absolutamente independiente, de modo que debe resultar inequívoca e independiente del resto del documento. Del mismo modo, se exige absoluta claridad en la declaración, Para ello, el legislador, utiliza varios términos diferentes de como modo de evitar confusiones y que confluyen en la certeza del interesado sobre el alcance de su consentimiento.

Así, en el caso de que la solicitud de consentimiento se realice por medios electrónicos "(…) *la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta*". Además, el consentimiento *"(…) debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines*"[442]. En consecuencia, cuando el tratamiento de datos tenga más de un fin, el consentimiento se deberá dar para cada uno de ellos, no aceptándose un consentimiento genérico.

Por otra parte, si lo analizamos desde una perspectiva negativa, en atención al Considerando 43, el consentimiento no puede considerarse otorgado libremente, cuando no exista un " (…) *equilibrio de poderes entre el interesado y el responsable y en particular cuando el responsable sea una autoridad pública*". Del mismo modo no podrá darse por válido el consentimiento cuando no puedan autorizarse de forma separada las diferentes operaciones del tratamiento de sus datos; ni cuando el consentimiento sobre el tratamiento de los datos haya sido exigido para el perfeccionamiento de un contrato, incluso cuando el mismo no sea requisito necesario para el cumplimiento de este. En todo

[442] Considerando 32 RGPD.

caso, esta presunción debe ser considerada como "*iuris tantum*" y por tanto admitirá prueba en contrario.

Sobre el tratamiento de datos en situación de desequilibrio, resulta interesante la posición del TS, que mantenía que, aquellos datos que no fueran en absoluto necesarios e imprescindibles para el mantenimiento y cumplimiento del contrato de trabajo no pueden verse amparados por la excepción de recabar el consentimiento prevista en el art. 6.2. LOPD; por lo que, para tratar el dato de correo electrónico personal de trabajadores con la finalidad de remitirles información sobre el pago de su nómina era necesario previamente contar con su consentimiento[443].

3. "*El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo*."

El derecho a la protección de los datos personales es considerado, como hemos visto, como un derecho fundamental, conformado esencialmente por la facultad de cada individuo de controlar el tratamiento de sus datos, por lo que este puede revocar en cualquier momento y a su exclusivo arbitrio el consentimiento otorgado anteriormente. No obstante, debe tenerse en cuenta que la revocación no es retroactiva, por lo que la decisión se aplica desde el día de la revocación, manteniendo lícito el tratamiento que hubieran sufrido los datos entre el consentimiento y la revocación del mismo.

Por ello, para hacer efectivo dicho derecho, en forma plena, este apartado no solo faculta al interesado a retirar su consentimiento, sino que, además, establece la obligación para quienes traten los datos, de facilitar los medios para la retirada o revocación del mismo, sin que el responsable pueda aplicar sanciones gravosas que imposibiliten o dificulten tal decisión, igualando las condiciones para retirarlos como para otorgarlo; ya que, como hemos visto, para el TC, "(…) *el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos (…) que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos*

[443] STS de 21 de diciembre de 2015.

personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer"[444].

Y, precisamente, entre estos deberes se encuentra el derecho a requerir el previo consentimiento del afectado para el tratamiento de sus datos, y, por tanto, de facilitarle los medios para revocar el consentimiento otorgado previamente.

4. "*Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato*".

Como señaló el GT29[445] al analizar esta situación, el legislador europeo aspira a garantizar que el consentimiento del interesado no sea convertido directa o indirectamente en la contraprestación de un contrato; aun cuando el tratamiento de datos no sea inevitable para la ejecución de este. Por ello, es absolutamente necesario analizar: si la aceptación de los términos y condiciones objeto del consentimiento se encuentran asociadas; así como si este se halla infundadamente asociado o ligado al perfeccionamiento de un contrato o un servicio cuando los datos personales solicitados no fueran necesarios para la ejecución o cumplimiento del contrato o para la prestación efectiva del servicio. En consecuencia, en caso de verificarse que existe esta asociación o vinculación, el consentimiento se podrá considerar condicionado y por tanto que no cumple con el principio de libertad de consentimiento.

2.3.2.3. Otras bases legitimadoras del tratamiento de datos de salud: el interés público

Como decíamos anteriormente, en el caso de datos especialmente protegidos, el tratamiento está dotado de un régimen de protección más estricto, como se contenía igualmente en la LOPD, que, no obstante, nos puede seguir ilustrando y ayudando a una

[444] STC 254/1993.
[445] Directrices del GT29 sobre el consentimiento en el sentido del RGPD, adoptadas el 28 de noviembre de 2017.

mejor interpretación de la regulación actual. Así, conforme al art. 7 LOPD, respecto de los datos que se refieren al origen racial, a la salud y a la vida sexual, se requiere el consentimiento expreso del afectado, y para los datos que revelen la ideología, afiliación sindical, religión y creencias afectado, se requiere el consentimiento expreso y por escrito del afectado; quedando exceptuado los ficheros de partidos políticos, sindicatos, iglesias y confesiones religiosas y asociaciones y entidades sin ánimo de lucro.

No obstante, el apartado. 6 LOPD excepcionaba de recabar el consentimiento, cuando fuera necesario para la prevención, diagnóstico médico, prestación de la asistencia sanitaria, el tratamiento médico o la gestión de servicios sanitarios; siempre que el tratamiento lo realice un profesional obligado a guardar secreto, además de cuando sea necesario salvaguardar el interés vital de afectado o de otra persona y se encuentre física o jurídicamente incapacitado para prestar el consentimiento.

Del mismo modo, el art. 6., desarrollado en el art. 10 RLOPD, contenía un conjunto de situaciones en las que no era necesario el consentimiento:

a) la existencia de una norma con rango de ley o de derecho comunitario y que: o bien el tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 LOPD; o bien que el tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas;

b) que los datos se recojan para el ejercicio propio de las AAPP en el ámbito de sus competencias;

c) que los datos se recaben con ocasión de un contrato o precontrato o de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento;

d) en el caso de que el tratamiento de datos tenga por finalidad el interés vital de interesado.

A ello, habría que añadir la situación derivada de que los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para satisfacción del interés legítimo del responsable del fichero o por el tercero al que se le comuniquen los datos (apdo. art. 6).

Estas excepciones de la LOPD y el RLOPD vienen a ser coincidentes en cuanto a su contenido con las previstas en el RGPD y la LOPDGG. Así, el art. 9.2 RGPD contiene otros supuestos de licitud del tratamiento de datos de salud (de categorías especiales de datos personales), que se excepcionan de la prohibición de tratamiento de estos datos del art. 9.1 RGPD.

Por ello, el apartado 2.b) del art. 9 RGPD, puede tener aplicación en el tratamiento de categorías especiales de datos en el contexto de la seguridad social y de los servicios sociales, que puede estar conectados con la asistencia socio-sanitaria, derivada de la exigencia de este precepto de que "el tratamiento (sea) 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".

El apartado 2.c) del art. 9 RGPD establece que "el tratamiento (sea) 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", en la que se pone de manifiesto la trascendencia y preferencia del derecho a la vida, que puede aplicarse perfectamente al ámbito de la salud, sin perjuicio de que disponga de otras habilitaciones más directas y específicas amparadas por la legislación sanitaria (LBAP, entre otras).

El apartado 2.e) del art. 9 RGPD contempla el supuesto de que "el tratamiento se refiera a datos personales que el interesado ha hecho manifiestamente públicos"; siendo posible el tratamiento de datos de salud una vez han sido hechos públicos por el interesado a través de los distintos medios de comunicación o difusión, incluidas las redes sociales de carácter abierto.

El apartado 2.g) del art. 9 RGPD se refiere al supuesto de que "el tratamiento (sea) 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".

En este caso, se habilita el tratamiento de categorías especiales de datos, y en especial de datos de salud relacionados con una actividad de contenido no sanitario, necesitándose una ley que habilite los tratamientos, como, para los seguros de salud[446], el control de alcoholemia derivado de la normativa de tráfico[447], o, dentro de la medicina deportiva, los controles antidopajes[448].

Por su parte, la LOPDGDD, salvo la regulación del art. 9 destinada a exigir que el consentimiento sea explícito, no establece regulación concreta alguna sobre el tratamiento de datos especialmente protegidos; de forma que se aplican los criterios de legitimación de categorías especiales de datos del art. 9. 2 RGPD. Sin embargo, sí se refiere al tratamiento de datos de salud (mediante el acceso a información administrativa), junto a datos genéticos o biométricos, entre otros, en la medida en que exista una ley habilitante, como señalábamos anteriormente, la Ley de Cohesión y Calidad del Sistema Nacional de Salud.

Los últimos apartados del art. 9. 2, h), i) y j) se refieren al tratamiento de categorías especiales de datos personales relacionados con el ámbito sanitario; es decir, la asistencia sanitaria, la salud pública y la investigación en salud y biomédica; que pueden ser considerados, de la misma forma que para los tratamientos por razón de interés público esencial, del apartado g), por el Derecho de la Unión o de los Estados miembros. La habilitación para el tratamiento de este tipo de datos está basada en una norma con rango de ley, que debe adecuarse al principio de proporcionalidad, en cuanto que "debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de

[446] Ley 20/2015, de 14 julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

[447] Real Decreto Legislativo 6/2015, de 20 de octubre, por el que se aprueba el Texto Refundido de la Ley sobre Tráfico, Circulación de vehículos a motor y Seguridad vial.

[448] Ley Orgánica 3/2013, de 20 junio, de protección de la salud del deportista y lucha contra el dopaje en la actividad deportiva.

datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

De esta forma, vemos como el nuevo régimen de cesión de datos, auspiciado por el RGPD y la LOPDGDD no ha alterado sustancialmente el régimen existente anteriormente, en cuanto a la necesidad de consentimiento, observándose un mayor rigor en su exigencia, en supuestos como el propio de la salud pública, cuya ley[449], excluye la necesidad de consentimiento en el tratamiento de datos personales relacionados con la salud o epidemiológicos, incluida la cesión entre administraciones públicas, cuando ello resultara estrictamente necesario para la tutela de la salud de la población y por razones imprescindibles. Sin embargo, tratándose de estudios científicos derivados de los datos de salud, la no necesidad de consentimiento se circunscribe únicamente al supuesto de tratarse de "situaciones de excepcional relevancia y gravedad para la salud pública"[450]; cuya determinación corresponde a las autoridades sanitarias, de acuerdo con las competencias atribuidas por la normativa aplicable.

Este no requerimiento de consentimiento del paciente para fines asistenciales por profesionales sanitarios, previsto por la Ley General de Salud Pública, choca, tanto con la prohibición general de tratamiento de los datos personales sin el consentimiento del interesado (como hemos visto), como de alguna forma, con el principio general de la LBAP[451] de exigencia del consentimiento (informado) del paciente; tanto verbal (con carácter general), como escrito (existiendo causas de riesgo)[452], como requisito previo para cualquier actuación en el ámbito de la salud. Resultando que ambos tipos de consentimiento resultan incompatibles[453].

[449] Art. 41 de la Ley 33/2011, de 4 de octubre, General de Salud Pública.
[450] Disp.Adic. 17ª LOPDGDD.
[451] Art. 8.
[452] "Intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente".
[453] TRONCOSO REIGADA, A., *La protección de datos sanitarios: La confidencialidad de la historia clínica, Protección de datos personales para servicios sanitarios públicos*, *op.cit*., p. 56.

2.3.2.3.1. El interés público como base legitimadora del tratamiento de datos de salud

Desde el ámbito de la salud, en el que nos encontramos, al margen del consentimiento y de otras bases, -como por ejemplo el cumplimiento de una obligación legal, art. 6.1.c) (para el empleador en la prevención de riesgos laborales de sus empleados)-, coexisten en el RGPD dos fundamentos o bases legitimadoras del tratamiento de datos: la existencia de una misión realizada en interés público (art. 6.1.e) y los intereses vitales del interesado u otra persona física (art. 6.1.d), el cual será objeto de análisis en el siguiente apartado.

Sin embargo, como indicaba en el apartado anterior (señala la AEPD[454]), para el tratamiento de datos de salud no es suficiente con la base jurídica del art.6 RGPD, sino que, como exigen los arts. 9.1 y 9.2 RGPD, es preciso una circunstancia que levante la prohibición de tratamiento de esta categoría especial de datos (entre ellos, los de salud). Y, así, estas circunstancias se encontrarían en el art. 9.2 RGPD. A saber:

1. En la letra "b)", relativa a las relaciones entre empleador y empleado. La cual, traslada a la situación actual de epidemia, 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).

2. En las letras "g) e i)", las cuales 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 cualificado "en el ámbito de la salud pública".

3. 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.

[454] AEPD, Informe N/REF: 0017/2020.

4. Y, en la letra "c)", en el caso de que se den las circunstancias previstas en este apartado, por lo que se 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.

Así, la existencia del interés público, como base legítima de tratamiento; que, como exige la LOPDGDD[455], "(…) *deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad*". Por ello, tratándose de datos de salud, es la Disp.Adic.17ª LOPDGDD la que relaciona las leyes que sirven a dicho amparo; siendo básicamente las aplicables al ámbito de la asistencia sanitaria la LGS, la LBAP y la Ley de Cohesión y Calidad del Sistema Nacional de Salud.

Además, tratándose de situaciones de riesgo sanitario como la que estamos padeciendo actualmente por la epidemia mundial del Coronavirus, se disponen de las medidas legales incluidas, en 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, y en la Ley de Salud Pública, cuyo art. 3 establece que: "*(…) con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible".* Además, en su art. 14 se autoriza el tratamiento de datos de salud o epidemiológicos sin necesidad de consentimiento, si ello es estrictamente necesario para controlar la salud de la población. Por su parte, los arts. 5 y 84 de dicha ley, prevén la posibilidad de poder adoptar medidas adicionales en caso de riesgo de transmisión de enfermedades (como el que padecemos).

Con carácter más genérico, el propio RGPD[456] reconociendo el carácter específico de los datos de salud, prevé la posibilidad de que los Estados miembros establezcan condiciones

[455] Art. 9.2. LOPDGDD.
[456] Art. 9.4. RGPD.

adicionales o incluso limitaciones al tratamiento de estos datos. Por ello, el apartado 2º habilita a los Estados miembros a mantener o introducir limitaciones más específicas, (que en todo caso han de perseguir un interés público y ser proporcionales al fin perseguido en relación con cada tratamiento) a fin de adaptar las normas sobre la licitud del tratamiento fijadas en el Reglamento; no sólo en los casos en que dicho tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable, sino cuando es necesario en cumplimiento de una misión realizada en interés público, por el ejercicio de poderes conferidos al responsable del tratamiento. Al mismo tiempo, esta habilitación se lleva a cabo con la finalidad de que se establezcan "(…) *de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX*"[457].

Las razones habilitantes del tratamiento en base al interés público se concretan normativamente en base a las siguientes razones[458]:

"g)" cuando 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.

Además, se exige que "*La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento* (…)"[459].

"i)" 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,

[457] PUYOL MONTERO, J., "Los principios del derecho a la protección de datos", en *Reglamento General de Protección de Datos…, op.cit.*, pp.141 a 145.

[458] Siguiendo el orden alfabético de los apartados del art. 9 RGPD.

[459] Art. 6.3.b) RGPD:

"(…) entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido".

o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios; lo que incluye todo lo relacionado con la protección y cuidado de la salud. Así, quedan comprendido "(…) *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 (…)".*

Sin embargo, en aplicación 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 deja claro que, ello, no debe dar lugar a que terceros, como empresarios, compañías de seguros o bancos, traten datos personales con otros fines; debiendo estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas[460].

En el ámbito de la salud, y en especial tratándose de salud pública, nos referimos a la actual situación de epidemia de coronavirus (COVID-19), en la que la propia AEPD ha señalado que durante la misma debe seguir procediéndose al tratamiento de datos personales respetándose todos sus principios y, especialmente, el de minimización de datos; de forma 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".*

[460] Considerando 54 RGPD:
"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. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.o 1338/2008 del Parlamento Europeo y del Consejo (1), es decir, 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. 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".

A propósito de la base legitimadora de "la salud pública", la AEPD ha emitido un comunicado como consecuencia de la epidemia del Coronavirus, señalando que esta epidemia no puede significar una suspensión del derecho fundamental a la protección de datos, y que, al mismo tiempo, su normativa reguladora no puede suponer un entorpecimiento de la asistencia sanitaria en esta situación, por lo que habrán de adoptarse soluciones que permitan compatibilizar de forma ponderada las medidas que se adopten con un uso lícitos de los datos personales[461].

Al mismo tiempo, recuerda la AEPD, que "las únicas finalidades para las que pueden tratarse los datos son las relacionadas con el control de la epidemia, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo. Además, los datos que puedan obtenerse y utilizarse han ser los que las autoridades públicas consideren proporcionados/necesarios para cumplir con dichas finalidades"[462].

Ya vimos en el apartado 2.2 el acceso a la historia clínica. Pues bien, como complemento de ello, en relación con el art. 7.6 de la LOPD (que suponía una reproducción del art. 8.3 de la Directiva 95/46/CE), el GT29[463] en un informe sobre los historiales médicos electrónicos, señalaba como la excepción de no necesidad de consentimiento del interesado cubre el tratamiento de datos personales para la finalidad específica de proporcionar servicios relativos a la salud de carácter preventivo, de diagnóstico, terapéutico o de convalecencia, así como para la gestión de estos servicios sanitarios, como la facturación, contabilidad o estadísticas. Sin embargo, queda fuera el tratamiento posterior que no sea necesario para la prestación directa de dichos servicios, como la investigación médica, el reembolso de gastos por un seguro de enfermedad o las reclamaciones económicas, además de lo que constituye la salud pública y la protección social.

Además, este tratamiento deberá ser necesario para los fines específicos incluidos en el apartado a) del art. 8 de la Directiva, por lo que habría que justificar plenamente cualquier

[461] Como igualmente se indica en el informe N/REF: 0017/2020 de la AEPD.
[462] AEPD, Comunicado con ocasión del Coronavirus, de 26 de marzo de 2020.
[463] GT29, Informe de 15 de febrero de 2007.

inclusión de datos personales en una HCE, ya que la simple utilidad de disponer de dichos datos no sería justificación suficiente.

Otra condición del tratamiento de datos personales es que deba ser realizado por un profesional sanitario o por otra persona sujeta al mismo secreto (médico) o profesional o a una obligación equivalente de secreto, "(…) *estando restringido a los facultativos que realizan el tratamiento médico y a las terceras personas, entre las que se incluyen los facultativos que no intervienen en el tratamiento, personal sanitario y social, de administración, etc., que puedan demostrar un uso legítimo (...)"*[464].

3. ANÁLISIS CRÍTICOS DE ALGUNOS TRATAMIENTOS DE DATOS DE SALUD

3.1. SITUACIONES DE URGENCIA VITAL

A la vista del abultado número de excepciones a la necesidad de consentimiento para el tratamiento de datos especialmente protegidos recogidas en el art. 9 RGPD, resulta novedoso la posibilidad que se concede a los Estados de la UE de mantener e introducir de forma específica condiciones adicionales, incluso mediante el establecimiento de limitaciones, en relación al tratamiento de los datos genéticos, biométricos, o los datos relativos a la salud, en general[465].

Así, en cuanto a las excepciones a la prohibición de tratamiento datos especialmente protegidos, las razones de interés vital, la anterior LOPD lo condicionaba, como veíamos, a que 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.

[464] Grupo de Trabajo de Ética de la Ciencia de las Nuevas Tecnologías, dictamen para la Comisión Europea, de 30 de julio de 1999.
[465] PUYOL MONTERO, R.," Los principios del derecho a la protección de datos", en *Reglamento General de Protección de Datos…, op.cit.*, pp.145 a 148.

En principio, no parece que existiera mucha conexión entre los datos de salud, que son los que tienen una incidencia directa sobre el interés vital de la persona, con los de ideología, afiliación sindical, religión o creencias, al relacionarse ambos según la dicción del apartado 6; salvo, quizás el ámbito de los Testigos de Jehová y su relación con la asistencia sanitaria en cuanto a sus creencias de no transfusión sanguínea. Por ello, la LOPD no aclaraba suficientemente que habría de entenderse por interés vital. No obstante, no caben dudas de su relación con el estado de salud de una persona y la necesidad de realización de las intervenciones sanitarias precisas para procurar la salud de la persona[466].

Doctrinalmente se entiende que el concepto de urgencia vital estaría compuesto de tres elementos: la gravedad, al existir un riesgo cierto de integridad o menoscabo de la vida, la urgencia o necesidad de intervención inmediata y la imposibilidad de que el paciente manifieste su voluntad en relación con la intervención sanitaria necesaria[467].

Para el TS, la apreciación de la situación de urgencia vital requiere la concurrencia de varios elementos:

1º.- Es necesario que se dé una situación de riesgo. Al mismo tiempo, no toda urgencia tiene carácter vital, sino únicamente aquella "(…) *que es más intensa y extremada y que se caracteriza, en los más de los casos, porque en ella está en peligro la vida del afectado* (…). Sin embargo, aunque en términos menos graves cabe apreciar la urgencia vital " (…) *ante la concurrencia de un peligro que dificulte la curación definitiva del enfermo o que provoque la pérdida de órganos o miembros fundamentales para el desarrollo normal del vivir, aunque la lesión se halle en una zona periférica del cuerpo. Y ello porque la urgencia vital no puede limitarse al "peligro inminente de muerte". porque tal conclusión no se desprende de la interpretación literal del precepto, máxime teniendo en cuenta que el mandato constitucional sobre el derecho de protección a la salud (art. 43.1 CE) "no permite una interpretación mezquina del precepto que nos ocupa" (STS*

[466] Entiende TRONCOSO REIGADA, A., que el interés vital se justifica en la vertiente objetiva del derecho a la vida que anima toda gestión asistencial y que prevalecería sobre el derecho a la intimidad y la protección de datos personales, *La protección de datos sanitarios: La confidencialidad de la historia clínica*, *Op.cit*., p.54.

[467] ARRUEGO, G., "La naturaleza constitucional de la asistencia sanitaria no consentida y los denominados supuestos de "urgencia vital", *Revista Española de Derecho Constitucional*, nº 82, 2008, p.80.

20/10/03)". De ahí, que la integridad moral suponga un concepto que está incluido en el término "vital"; por lo que, es preciso *la existencia de "(...) una situación patológica que presuntamente ponga en peligro la integridad fisiológica del enfermo"*.

2º.- Que se trate de una situación de riesgo objetiva y contrastada[468].

3º.- Que el riesgo sea inesperado e imprevisible, (…) *como un accidente o la aparición súbita de un cuadro clínico que requiera de una inmediata atención"*[469].

4º.- Que exista perentoriedad o premura en la actuación, en la medida de que (…) *se perjudica la supervivencia del enfermo o se le puede infligir un daño irreparable o de difícil subsanación a su integridad física si ha de estarse a la necesaria demora o a la superación de los naturales inconvenientes que supone el acudir a los servicios médicos asignados por la Seguridad Social"*.

Y esta perentoriedad significa, en consecuencia, (…) *la exigencia de tratamiento inmediato ante la aparición imprevisible de la enfermedad o la producción del accidente y que elimina o excluye cualquier posibilidad de trámites formales y burocráticos previos, de modo que resulte ineludible acudir al centro más cercano de los adecuados*[470]*. O que sea extremadamente dificultoso o desaconsejable médicamente el acudir a los servicios sanitarios propios de la Seguridad Social*[471]*. O requiera una atención inmediata"*[472].

El GT29 se pronuncia en relación al concepto de "interés vital del interesado", señalando su carácter restrictivo; de forma que "El tratamiento debe referirse a intereses individuales esenciales del interesado o de otra persona, y debe -en el contexto médico- ser necesario para un tratamiento médico dirigido a salvar la vida en una circunstancia en que el interesado no esté en condiciones de expresar sus intenciones. Por consiguiente, esta excepción sólo puede aplicarse a un número reducido de casos de tratamiento, sin que pueda utilizarse para justificar el tratamiento de datos médicos personales con fines

468 SSTS de 22-10-1987, 16-2-1988, 14-12-1988, 1-7-1991 y 31-5-1995.
469 SSTS de 9-7-1986, 15-1-1987, 9-6-1988 y 25-10-1999.
470 SSTS de 15 de enero de 1987 y 1 de julio de 1991.
471 STS de 7-3-1985.
472 STS de 25-10-1999.

distintos al tratamiento del interesado, como serían la realización de investigaciones médicas de ámbito general que sólo en el futuro darán resultados"[473].

El Considerando 46 RGPD se refiere al término "interés esencial" para la vida del interesado o de otra persona física, de forma que, "(…) *en principio, los datos personales deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente*". Alude, además, a motivos conjuntos de interés público e interés vital que pueden justificar el tratamiento excepcional de datos, tales 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 su parte, el art. 9 RGPD[474], incluye dentro de las excepciones a la prohibición de tratamiento datos especialmente protegidos, las razones de interés vital, en el caso de que "(…) *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*" (apartado c). Al mismo tiempo el art. 6.1.d) considera suficiente base jurídica (lícita) de tratamiento el interés vital de interesado[475], así como de otras personas físicas; por lo que puede incluso incluir a personas no identificadas o identificables.

Lo anterior, nos lleva a concluir, para su aplicación a la indicada situación actual de epidemia que, 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

[473] En el documento 00323/07/ES WP 131, de 15 de febrero de 2007, se señala que, supongamos que un interesado ha perdido la consciencia después de un accidente y no puede dar su consentimiento para la revelación necesaria de alergias conocidas. Estando en el contexto de un historia médica electrónica, supone que esta excepción permitiría a otro profesional de la salud acceder a la información almacenada en la historia clínica a fin de obtener datos sobre alergias conocidas del interesado, que pueden resultar decisivas para el tratamiento realizado.

[474] En una regulación muy similar a la del art. 8.2.c) de la Directiva 95/46/CE.

[475] Configurado como persona física identificada o identificable, según el art. 4.1. RGPD.

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*''*[476].

Señalar, que esta base de tratamiento (art. 6.d) no necesita ser establecida por el Derecho de la Unión o el Derecho de los Estados Miembros aplicables al responsable del tratamiento, ya que este requisito rige exclusivamente para el tratamiento derivado del cumplimiento de una obligación legal o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos (apartados c) y e) del art. 6), pero no para el tratamiento incluido en la letra d).

3.2. UTILIZACIÓN DE DATOS DE SALUD POR COMPAÑÍAS ASEGURADORAS

La Ley de Contrato de Seguro[477], establece el deber del tomador del seguro de declarar al asegurador todas las circunstancias que conozca que puedan tener influencia en la valoración del riesgo. Por tanto, antes de la firma del contrato y durante la vigencia del mismo, debe comunicarse al asegurador las circunstancias agravantes o atenuantes del riesgo cubierto por el seguro; pudiendo aquel modificar o rescindir el contrato por agravación del riesgo (arts. 10 a 13).

Siguiendo el informe de la AEPD[478], señala la no aplicación a los datos de salud de la doctrina del interés legítimo[479], así como la aplicación directa del art. 7.f) de la Directiva 1995/46/CE, consagrada por la STJCE de 24 de noviembre de 2011; distinguiendo, al mismo tiempo, tres situaciones diferenciadas:

a) Supuesto de que, con motivo de la contratación de un nuevo seguro, o circunstancia equivalente, se conocieran datos "preexistentes" al primer contrato celebrado.

En este sentido, en aplicación del art. 4 LOPD y el art. 8 RLOPD, e indirectamente según el art. 94.2 LOPDGG, resulta que los datos de carácter personal sólo podrán ser recogidos

[476] AEPD, Informe N/REF: 0017/2020.
[477] Ley 50/1980, de 8 de octubre, de contrato del Seguro.
[478] AEPD, Informe N/REF: 0452/2012.
[479] Al que se refiere el Considerando 47 RGPD.

para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento, y estas finalidades son sólo aquellas "para las que se hayan obtenido". En este caso, para los fines de un determinado contrato de seguro y no para otros diferentes.

La AEPD, tuvo ocasión de tratar este asunto en los siguientes términos: *"*Dado que el consentimiento del asegurado para el tratamiento de estos datos, se recaba para la finalidad concreta de desenvolvimiento de la relación de seguro y gestión de los siniestros (fallecimiento, incapacidad permanente total o incapacidad temporal por enfermedad o accidente), debe recordarse el principio de proporcionalidad y necesidad del artículo 4 de la LOPD en la recogida y tratamiento de los datos personales, de modo que sólo se podrán recoger y tratar cuando sean adecuados, pertinentes y no excesivos en relación con la finalidad señalada, no pudiendo usarse para finalidades diferentes de las que motivaron la recogida y para la cual se solicita el consentimiento*"*[480].

En el ámbito sanitario, la adecuación y pertenencia supondría que, por ejemplo, un paciente que va a ser tratado de una enfermedad pulmonar el médico, por su posible influencia en su patología, pueda hacer un seguimiento de su hábito de fumador, pero no será admisible que pueda accederse a su nivel de estudios o de renta.

b) Supuesto de celebración de un segundo contrato o, bien por motivos distintos, en el que después de firmado se conocen nuevos datos.

En este caso, la AEPD entiende que, los arts. 11 a 13 de la Ley de contrato de seguro y su relación con el art. 7.3 LOPD, implican una habilitación legal suficiente para el tratamiento de los datos de salud y su aplicación a contratos posteriores; además de que el contenido de dichos datos de salud puede suponer una agravación o minoración del riesgo a asumir por el asegurador.

c) Tratándose del supuesto de que la compañía aseguradora tiene conocimiento de datos de salud como consecuencia de la celebración de un segundo contrato todavía sin celebrar.

[480] AEPD, Informe de 28 de mayo de 2010.

Aquí la AEPD entiende que no es preciso acudir a la habilitación legal de la Ley de contrato de seguro y el art. 7.3 LOPD, habida cuenta de que la propia legislación en materia de seguro prevé la posibilidad de que el tomador pase un reconocimiento médico, si entendiera que existe una agravación del riesgo inicial.

En relación con la cesión de datos de salud a las compañías de seguros por los centros sanitarios, habría que distinguir:

a) Si se trata de la comunicación de datos del centro sanitario al asegurador para dar cumplimiento al pago de las indemnizaciones procedentes, es posible dicha comunicación;

b) Sin embargo, si se trata de asistencia sanitaria, es preciso el consentimiento del asegurado en la firma de la póliza, además de para cada acto médico.

Como caso excepcional, los datos pueden comunicarse conforme al principio de calidad, exclusivamente con la finalidad de elaborar la factura del gasto sanitario. De forma que, sólo se cederán los que resulten adecuados, pertinentes y no excesivos para poder determinar el importe de dicha asistencia sanitaria; necesitándose la previa firma de un contrato de destinatario de datos entre la aseguradora y el centro sanitario o profesional privado, conforme al art. 24 RGPD; correspondiendo la responsabilidad deriva del correcto tratamiento de datos al encargado del tratamiento, por cuenta y bajo las instrucciones del responsable del tratamiento. Recordar, como en el apartado 2.3.1.3. hemos tratado la problemática de las figuras del responsable-encargado y del corresponsable, de tratamiento de datos personales.

3.3. ACCESO A DATOS DE SALUD POR SERVICIOS EXTERNALIZADOS

En el ámbito de la externalización de servicios sanitarios públicos (como pruebas diagnósticas, de laboratorio, tratamientos médicos, etc.), mediante concesión, encomienda de gestión o contrato a un centro sanitario privado, la LOPD no los consideraba cesión de datos en sentido estricto y, por tanto, no necesitada del consentimiento del interesado, y se concebían como meros accesos para la prestación de un servicio al responsable del tratamiento; para lo cual resultaba necesario la

formalización de un contrato entre el responsable del tratamiento y el encargado de realizar la prestación.

La AEPD[481] se refería a la aplicación a este caso de lo dispuesto en el art. 7.6 LOPD[482], y al art. 8, que establecía que:

"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"; junto con la obligación de guardar el secreto profesional sobre los datos del responsable del fichero y de quienes intervengan el cualquier fase del tratamiento de los datos de carácter personal, subsistiendo dicha obligación aún después de finalizada la relación (art. 10).

Sin que se considere comunicación de datos "(..) *el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento"* (art. 12).

Ello, además de exigir que*, "La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato…*", por el RLOPD, en el que el subcontratado no pueda utilizar los datos para otros fines, ni comunicarlos a otras personas; comprometiéndose a adoptar las medidas de seguridad legalmente previstas y a devolver o destruir los datos una vez cumplida la prestación, en cuyo caso los casos deberán permanecer bloqueados.

Sin embargo, la nueva LOPDGDD no se ocupa con profundidad de abordar las relaciones entre el responsable y el encargado de tratamiento, sólo se refiere de a las medidas de seguridad, al señalar que "*En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se*

[481] AEPD, Informe 248/2005.

[482] Art. 7.6. LOPD:

"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".

*corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad" (*Disposición Adicional segunda).

De esta forma, habrá que acudir a la otra fuente normativa, el RGPD para conocer cómo se llevan a cabo estas relaciones entre responsable y encargado del tratamiento. Así, el art. 6 RGPD considera lícito el tratamiento cuando, además de en el caso de que se haya prestado el consentimiento, se den alguna de las condiciones que legitiman el mismo. Así, se encuentra la de que "*el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte*" (apartado b), y que ha sido objeto de tratamiento específico en el apartado 2.3; referido al responsable-encargado del tratamiento, contemplándose, incluso, la posibilidad de un tratamiento conjunto de datos cuando dos o más responsables del tratamiento determinen conjuntamente los objetivos y establezcan los medios del tratamiento necesarios para el mismo (corresponsable del tratamiento).

4. SEGURIDAD DE LOS DATOS SANITARIOS

La seguridad en el tratamiento de los datos personales constituye, además de una obligación, un principio del tratamiento, debiendo acomodarse al tipo o categoría de datos que se trate. Así, los datos "(…) *serán tratados de manera que se garantice una seguridad adecuada, 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*"[483]; las cuales deberán ser adoptadas por el responsable del fichero y, en su caso por el encargado del tratamiento; de forma que, "(…) *garanticen la seguridad de los datos de carácter personal, considerando el estado de la técnica, la naturaleza y los riesgos de los datos almacenados…habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos.*"[484].

[483] Art. 5.1.f) RGPD.
[484] Art. 32 RGPD.

Al mismo tiempo, el tratamiento debe garantizar la integridad y confidencialidad de los datos tratados, ya que "(…) *los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento*"[485].

4.1. RIESGOS EN LA PROTECCIÓN DE LOS DATOS SANITARIOS

Ya hemos visto como los datos sanitarios contienen un conjunto de información sobre el estado de salud de una persona, que incluye las pruebas y tratamientos recibidos y demás aspectos del proceso asistencial del paciente, y que, a pesar del empeño de los profesionales sanitarios implicados en dicho proceso, pueden verse comprometidos, quebrándose la confidencialidad y surgir brechas de seguridad que saquen a la luz aspectos íntimos de la persona que pueden hacerla vulnerable.

Así, podemos señalar, entre otros, los riesgos a los que se enfrenta diariamente la protección de los datos sanitarios:

a) Existencia de filtraciones interesadas e intencionadas provenientes de personal del propio centro sanitario.

b) Robo masivo de datos por parte de organizaciones que los utilizan para comercializar con ellos.

c) La propia negligencia de los usuarios autorizados, al no respetar los protocolos y las medidas de seguridad establecidos. En este sentido resulta fundamental la actuación a nivel personal que se lleve a cabo y, en concreto en el ámbito de las llamadas ciberamenazas.

[485] Considerando 39 RGPD.

4.2. SUPERVISIÓN DEL TRATAMIENTO DE DATOS DE SALUD: DELEGADO DE PROTECCIÓN DE DATOS[486]

Dentro de determinadas empresas deberá existir un DPD, que será el responsable de la supervisión del tratamiento de los datos personales, así como de informar y aconsejar al resto de los trabajadores de la empresa o centro sanitario que manejan datos de cuáles son sus obligaciones al respecto; siendo, además, el nexo entre dichos trabajadores y las autoridades sobre protección de datos. Esta figura, podrá ser trabajador (o funcionario) de la empresa (o Ente público), o ser contratado externamente para la realización de este cometido; aceptándose que recaiga también en una persona particular de dentro de la organización o al margen de ella.

El nombramiento de un DPD será obligatorio para toda empresa: que trate datos de salud o datos sensibles, o determinadas categorías de datos detallados en la norma; cuando la empresa supervise habitual o sistemáticamente a los ciudadanos; cuando la actividad principal de la empresa sea propiamente el tratamiento de datos o cuando el tratamiento de los mismos se efectúe a gran escala. Para el resto de las empresas el nombramiento del delegado es discrecional.

A modo de ejemplo, podríamos decir que, si los datos son utilizados con la finalidad de orientar a los algoritmos de los motores de búsqueda con la finalidad de publicidad, la empresa deberá tener un encargado del tratamiento; sin embargo, si los datos son utilizados por la empresa para enviar ocasional y directamente publicidad no será necesaria la figura del delegado. Una situación similar se da en el ámbito de la salud. Así, cuando un médico en su consulta privada recaba los datos del paciente y los utiliza simplemente a los efectos del control de la salud de este no necesitará un delegado; mientras que, si nos situamos en el ámbito de un hospital, resultará necesario a la vista de la cantidad y calidad de los datos manejados.

Entre las entidades y organismos que, de forma obligatoria, deberán designar un DPD, conforme al art. 34 LOPDGDD, destacamos:

[486] Para más información, tener en cuenta las consideraciones del GT29, Directrices sobre los delegados de protección de datos (DPD), Adoptadas el 13 de diciembre de 2016.

- 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.

No obstante, aquellas otras que lo consideren, podrán designar una delegado voluntario, sujeto a las prescripciones del Reglamento y la LOPDGDD; debiendo comunicarlo (además de los ceses), al igual que las entidades de obligada designación, a la AEPD en el plazo de diez días.

La LOPDGDD, señala que, en todo caso, se debe designar delegado de protección de datos en "*Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes*" (Letra l) del art. 34.1), excepto "*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*".

La designación del delegado corresponde únicamente al "*responsable del tratamiento o encargados del tratamiento"* (art. 34.1 de la LOPDGDD); y esta condición se les atribuye a los directores-gerentes de los centros sanitarios; que, por tanto, serán los encargados de su designación.

Del mismo modo, la LOPDGDD, obliga a que se designe un DPD en los Comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, o, en su defecto, un experto en el RGPD[487].

El RGPD, acoge esta figura en los arts. 37 a 39. Así, a la luz del art. 37, que prevé la posibilidad de un único DPD para varias autoridades u organismos públicos, nos planteamos, si, "*teniendo en cuenta su estructura organizativa y tamaño",* su aplicación a los Servicios regionales de salud resultaría procedente. La respuesta sería negativa a disponer de un único DPD por cada Servicio de salud de la Comunidad Autónoma, a la vista de las consideraciones antes expuestas de la necesaria existencia por cada centro sanitario. Sin embargo, parece existir cierta disparidad en relación con los modelos de DPD utilizados en el ámbito del SNS; así, mientras hay CCAA como Andalucía, Madrid

[487] Disp.Adic. 17ª, letra h) LOPDGDD.

o Asturias que disponen de su propio DPD, otras como Euskadi o Castilla-La Mancha han optado por un único DPD para toda la Administración autonómica. Por ello, parece que sería beneficioso que la AEPD se pudiera pronunciar al respecto. Aunque, en todo caso, la propia especificidad de la materia sanitaria: la singularidad de los datos de salud; la organización específica y compleja del SNS y de los Servicios regionales de salud; la cantidad ingente de información que manejan y tratan las direcciones-gerencias de los centros sanitarios, entre otras cuestiones, parecen argumentos de peso para apostar por que exista un DPD para sanidad, al margen de la necesaria existencia de los delegados de los centros sanitarios.

Con la finalidad de que empresas y entidades puedan contar con profesionales seguros y fiables, y pueden hacer una selección cualificada de profesionales, con competencias certificadas por ENAC, la AEPD ha promovido un Esquema de Certificación de PDP[488].

4.3. MEDIDAS DE SEGURIDAD Y VIOLACIÓN DE LA SEGURIDAD EN EL ÁMBITO SANITARIO

La seguridad de los datos supone una triple garantía: de la integridad de la información; de que ésta se encuentra disponible para su acceso por quien esté autorizado; además de suponer una garantía respecto de su confidencialidad.

El Reglamento ya no establece las medidas de seguridad por niveles o capas (como preveía la LOPD), sino que adopta el sistema preventivo del riesgo, previéndose que se apliquen medidas organizativas y de seguridad en función del riesgo que pueda acaecer en el tratamiento de datos. De esta forma, si el tratamiento de los datos de salud comporta un riesgo máximo será necesario diseñar que estas medidas se adecuen a la trascendencia de este riesgo. Así, la HC puede contener dos tipos de datos: los propios datos de salud, sujetos a un riesgo superior, sobre los que cabe aplicar la Evaluación previa de Impacto, y los datos de carácter personal, que pueden considerarse como datos no especialmente protegidos, en los que la previsión y evaluación del riesgo tendrían otro alcance.

[488] Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos (ESQUEMA AEPD-DPD) https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf.

La Evaluación de Impacto, consistente en un análisis de riesgo dirigido a que por los responsables del tratamiento se adopten las medidas adecuadas para reducir los riesgos, minimizando la probabilidad de materialización de los mismos y las afectaciones negativas a los interesados; correspondiendo realizarla al centro sanitario responsable del tratamiento, con el asesoramiento del DPD de protección de datos.

Constituye, por tanto, una herramienta de carácter preventivo que debe realizar el responsable del tratamiento dirigida a poder identificar, evaluar y gestionar los riesgos a los que están expuestos sus actividades de tratamiento, a fin de garantizar los derechos y libertades de las personas físicas; lo que en la práctica permite determinar el nivel de riesgo de un tratamiento con el fin de adoptar las medidas de control que permiten un nivel adecuado de riesgo[489].

Recordar, que el RGPD, incluye a los datos especialmente protegidos, y, por tanto, a los datos de salud, respecto de la necesaria realización de la evaluación del impacto que pudiera tener en cuanto al riesgo a los derechos y libertades de los titulares de datos de salud[490].

El responsable y encargado están obligados a mantener un registro de las actividades de tratamiento de datos de salud que realicen; el cual, como mínimo deberá contener la información prevista en el art. 30 RGDP.

Al hablar de la HC, en el apartado 2.2, ya comentamos la necesidad de preservar la confidencialidad de su contenido, mediante la adopción de diversas medidas de seguridad, que deben complementarse con las que ahora examinamos. Así, como señala la AEPD[491], el responsable del tratamiento de datos incluidos en la HC es el médico del centro sanitario público o privado, que tiene la obligación de elaborarla, cuidarla e implantar las medidas de seguridad necesarias para que no se extravíe o se acceda por terceros. Además "no es necesario que el médico o el centro sanitario solicite el consentimiento a los pacientes para la recogida y utilización de los datos personales y de salud si se van a utilizar para fines de medicina preventiva y laboral, para la evaluación

[489] AEPD, Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetos al RGPD. Mayo de 2018.
[490] Art. 35.3.b): "tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1".
[491] Guía de pacientes y usuarios de la sanidad, 2019.

de la capacidad laboral del trabajador, el diagnóstico médico, la prestación de asistencia, el tratamiento sanitario o la gestión de los servicios de asistencia sanitaria y social".

Dado que los datos deben ser exactos y actualizados, habrán de adoptarse "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"[492]. En la HC corresponde al profesional sanitario determinar los datos a suprimir o rectificar.

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 los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, corresponde a los profesionales médicos y a los propios centros sanitarios públicos y privados (a través del Director-Gerente o Director) adoptar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. En todo caso, las medidas deben garantizar la confidencialidad, integridad y disponibilidad de los datos, y en el caso de acaecimiento de un incidente de carácter técnico o físico, poderse restaurar el acceso y disponibilidad de los datos personales.

Entre las medidas a adoptar, entre otras estarían:

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, así como la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

c) Realizar un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) Disponer de un catálogo de medidas de seguridad reconocido en normativas o estándares de seguridad de la información.

Al evaluar la adecuación del nivel de seguridad, se tendrán en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de unas hipotéticas: destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos,

[492] *Ibid.*

conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Las partes intervinientes permitirán y contribuirán a la realización de auditorías, incluidas inspecciones, a la otra parte.

La ausencia o adopción anómala de medidas de seguridad puede entrañar violaciones de seguridad de los datos sanitarios, tales como "(…) *pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión*"[493].

En caso de violación de la seguridad de los datos personales en los sistemas de información utilizados por los intervinientes en la prestación de los Servicios sanitarios, deberá notificarse, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas hábiles, las violaciones de la seguridad de los datos personales a su cargo de las que tengan conocimiento; juntamente con toda la información relevante para la documentación y comunicación de la incidencia conforme a lo dispuesto en el artículo 33.3 del RGPD. Además, el responsable deberá comunicar las violaciones de seguridad de los datos a la Autoridad de Protección de Datos y/o a los interesados (si entraña un grave riesgo para los derechos y libertades de las personas físicas) conforme a lo establecido en la normativa vigente[494].

[493] Considerando 75 RGPD.

[494] Aplicación de lo previsto en el Considerando 85 del RGPD, que establece:
"Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida".

Se plantea sí sería posible facilitar información no presencial sino telefónica al titular de los datos sobre aspectos concretos de su estado de salud, como puedan ser los resultados de unas pruebas diagnósticas realizadas. Sin embargo, surge la posibilidad del riesgo de dar información a personas que no sean realmente los titulares de los datos, por lo que razones de seguridad aconsejan no utilizarlo. No obstante, podría establecerse un protocolo de seguridad, que incluya un conjunto de datos personales identificativos del titular de los datos, como nombre y apellidos, DNI, dirección, nº de tarjeta sanitaria, etc. que aseguren la identidad de quien realiza la llamada.

En el caso de la emisión por los centros sanitarios de justificantes de personas que acompañan a pacientes a un determinado acto médico, el acompañante tiene un interés legítimo para recibir el justificante, debiendo acreditar su vinculación con el paciente. En cuanto al contenido del justificante, por aplicación del principio de minimización de datos, sólo debe incluir el nombre y apellidos del paciente y la especialidad médica de que se trata, sin que aparezca la patología ni ningún tipo de información médica del paciente.

Tratándose de la identificación de profesionales sanitarios de centros privados y, por tanto, de un tratamiento de datos personales especialmente protegidos, éste resultaría amparado en el marco de ejecución de un contrato; aplicándose el principio de minimización, o de aportación de la información estricta que permita su identificación; por lo que, a fin de garantizar un trato personalizado con el paciente (sin perjuicio del deber de informar por parte del centro sanitario (art. 13 RGPD) podría utilizarse una tarjeta personal con sus nombres, apellidos y cargo en el centro; aunque para determinados servicios, como Urgencias, Psiquiatría o Salud Mental se suelen incluir las iniciales del especialista médico. La inclusión de una fotografía o número de DNI resultaría muy discutible, por lo que la realidad apunta a su no inclusión.

En relación con la indicada identificación de profesionales sanitarios, por parte de la AEPD se han realizado las siguientes Recomendaciones dirigidas a los directores de los centros sanitarios en general[495]:

[495] AEPD, Plan de Inspección sectorial de oficio en hospitales públicos. Septiembre 2017.

- No utilización de usuarios genéricos en la identificación y autentificación de datos sanitarios, salvo que, excepcionalmente se encuentren disociados mediante un código. Debe establecerse un mecanismo que permita la identificación inequívoca y personalizada de los accesos que se realicen, que deben quedar registrados, así como la comprobación de su autorización.
- Almacenamiento de las contraseñas de acceso de forma ininteligible.
- Limitación del número de intentos de acceso no autorizado al sistema, dando lugar al bloqueo del usuario.
- Realización frecuente de copias de respaldo (y en ubicación distinta) para todas las aplicaciones sanitarias.
- Anonimizar los datos utilizados en la realización de pruebas de software desarrollado.
- Realización, al menos cada dos años, de auditorías de seguridad sobre el cumplimiento de los ficheros con datos sanitarios.
- Debe procederse al cifrado de todas las comunicaciones de datos de salud que se realicen a través de redes públicas de telecomunicaciones, de forma que se garantice que la información no sea inteligible ni manipulada por terceros; por lo que debe rechazarse la comunicación de datos vía fax si no están cifrados. Sólo en el supuesto de que fuera imprescindible el envío por esta vía deberán disociarse previamente los datos.

  Tratándose del envío de datos sanitarios de riesgo alto, debería, igualmente, procederse a su disociación previa.
- En los mostradores de los espacios de los centros sanitarios destinados a información al paciente deben evitarse cualquier documentación que contenga datos personales.

4.3.1. MEDIDAS DE SEGURIDAD A ADOPTAR POR LAS ENTIDADES PÚBLICAS

Las distintas entidades públicas cuentan con medidas de seguridad, como la Política de Seguridad que gestiona y protege la información y los servicios públicos, en base al

Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad[496]; por lo que, además, deberán proyectar una Política Integral de Protección de Datos Personales en torno a una estructura organizativa liderada por el DPD[497], en la que se establezcan distintos niveles de responsabilidad, así como canales de comunicación entre el Delegado y los responsables del tratamiento.

En cuanto a la adopción de medidas de seguridad por el sector público, la Disp.Adic.1ª LOPDGDD señala:

"1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. 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.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad".

[496] Previsto en el art. 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y en el RD. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
Señala el indicado art. 156:
"1. El Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.
2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".

[497] Conforme al Considerando 81 RGPD, las Entidades Públicas, de cara a la aplicación de medidas técnicas y organizativas, deben recurrir únicamente a encargados que ofrezcan garantías, en particular en lo referente a conocimientos especializados, fiabilidad y recursos.

4.4. RESPONSABILIDAD PROACTIVA EN EL TRATAMIENTO DE DATOS DE SALUD

De acuerdo con el RGPD, corresponde al responsable del tratamiento dar cumplimiento a los principios relativos al tratamiento, previstos en el apdo.1 del art. 6, y que hemos analizado anteriormente, así como ser capaz de demostrarlo.

El RGPD, partiendo de una filosofía preventiva, contempla como en el tratamiento de datos personales ha de realizarse desde un planteamiento previo basado en el riesgo; que, por otra parte, ya la Directiva 95/46/CE preveía como criterio para determinar las medidas técnicas y organizativas a adoptar por el responsable del tratamiento, entre otros, respecto de categorías especiales de datos (art. 8), la seguridad del tratamiento (art. 17) y los controles previos (art. 20)[498].

De esta forma, el Reglamento, como una de sus novedades más importantes, introduce, con carácter general, la obligación del responsable del tratamiento de realizar "antes del tratamiento" una Evaluación del impacto (EIPD) previsto de las operaciones de tratamiento, entre otros supuestos, *"(…) 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 (*…)"[499].

En concreto, el art. 35.3 RGPD se refiere a la necesidad de la EIPD en el caso de:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1 (que incluye los datos de salud) o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10;

[498] RECIO GAYO, M., "Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a las autoridades de control", en *Reglamento General de Protección de Datos*…, *op.cit*., pp. 352 y ss.
[499] Art. 35.1 RGPD.

c) Observación sistemática a gran escala de una zona de acceso público.

Así, se parte de que, por principio, no existe esta obligación de realizar la EIPD si no estamos ante datos de carácter personal, aunque que, como medida de precaución en relación a preservar los derechos de los ciudadanos, se ha de considerar el concepto de "dato de carácter personal" establecido en el RGPD, de una forma extensiva, es decir, se ha de considerar que se tratan de datos de carácter personal por defecto y no asumir, a priori, que no se pueda dar dicha categoría a los datos tratados.

Para facilitar a los responsables de los tratamientos la identificación de aquellos tratamientos que requieren o que no requieren una EIPD, se han publicado de forma orientativa listas por parte de las autoridades de control. Así, la AEPD ha establecido una lista de tratamientos exentos de EIPD[500]; lo que no excluye la obligación de realizar las obligaciones impuestas en el RGPD[501].

[500] Basada en el documento WP 248, "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679".

[501] Lista publicada por la AEPD, 4 de septiembre de 2019, en la que no es necesario realizar Evaluación de Impacto:

"1. Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.

2. Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en particular la AEPD siempre y cuando una EIPD completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la EIPD.

3. Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.

4. Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.

5. Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.

6. Tratamientos realizados por comunidades y subcomunidades de propietarios tal como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.

7. Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento de datos sensibles tales como los que se establecen en el artículo 9.1 del RGPD y no sea de aplicación el artículo 9.2(d) de dicho Reglamento.

Por otra parte, basada en los criterios del GT29[502] se ha publicado una lista de tratamientos que si requieren EIPD. De esta forma, salvo que el tratamiento se incluya dentro de los que el art. 35.5 RGPD considera que no requieren EIPD, cuando el tratamiento cumpla con dos o más criterios previstos en dicha lista, deberá realizarse la EIPD, conforme al art. 35.4. RGPD; y cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD[503].

En el supuesto de que el responsable del tratamiento después de haber realizado la evaluación de impacto resulte que "(…) *el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo* (…)" habrá de consultar a la autoridad de control para que le asesore; la cual podrá utilizar cualquiera de sus poderes previstos en el art. 58; todo ello, en los términos del art. 35 RGPD.

Mediante esta obligación del responsable del tratamiento se pretende: mejorar el cumplimiento del Reglamento[504], dar cumplimiento al principio de responsabilidad proactiva, aumentar la transparencia para los interesados e incrementar la seguridad de los datos personales.

La aplicación del principio de responsabilidad proactiva exige la adopción por el responsable del tratamiento, con el asesoramiento del DPD, si existiera, de medidas organizativas y técnicas además de la aplicación de políticas internas que sean adecuadas para la protección de los datos personales desde "el diseño y por defecto" del riesgo para los derechos y libertades de las personas físicas, a fin de garantizar el cumplimiento de la normativa de protección de datos (art. 15 RGPD).

Al mismo tiempo, dichas medidas deberán, además de ser necesarias para la prevención de riesgos, demostrar que se cumple con la normativa de protección de datos personales,

[502] GT29 Guía W248 "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del RGPD", adoptadas el 4 de abril de 2017.

[503] Así, de acuerdo con la publicación de la AEP, requieren EIPD, entre otros los siguientes tratamientos: "(…)
4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.
6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin (…)".

[504] Vide Considerando 85 RGPD.

para lo que el responsable deberá adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto; debiendo estar actualizadas, para lo que deberán revisarse, si procediese. Las medidas están referidas a la protección de datos desde el diseño y por defecto (*Privacy by Design y Privacy by Default*); pudiendo consistir, entre otras, en "reducir al máximo el tratamiento de datos personales y seudonimizar lo antes posible los datos personales"[505].

La Directiva 45/96 ya recogía la "*accountability*"[506], en su art. 23, se refería al derecho al resarcimiento del responsable del tratamiento derivado de un tratamiento ilícito o contrario a la normativa sobre de protección de datos. Sin embargo, en el RGPD (art. 14) se pasa, de una responsabilidad pasiva derivada de la producción de un resultado dañoso en el tratamiento de datos personales, a una responsabilidad preventiva o proactiva, en la que, partiendo de que el tratamiento de datos personales implica un riesgo, como forma de prevenir posibles riesgos derivados del tratamiento de datos, incluye un conjunto de obligaciones a cumplir por el responsable, las cuales llevan aparejadas la adopción de medidas de seguridad acordes con la naturaleza, el contexto y los fines del tratamiento; por lo que, en conjunto, deberá desarrollar una planificación general y completa que asegure la observancia de la normativa sobre protección de datos personales.

Por su parte, la LOPDGDD, señala en el Preámbulo 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 sentido, cabe citar las palabras del profesor PIÑAR MAÑAS, señalando como el Reglamento, bien de forma directa o indirecta, introduce "un nuevo modelo de protección de datos para Europa, al pasar de la gestión de los datos al uso responsable de la información; siendo seguramente el cambio más profundo que va a imponer. Sin que

[505] Considerando 78 RGPD.

[506] Sobre su significado y alcance, ver el Dictamen 3/2010, W 173, de 13 de julio de 2010, emitido por el GT29.

estemos ante un modelo más sencillo que el anterior, aunque se deja mayor margen de valoración y apreciación a los responsables y encargados"[507].

En este sentido, el art. 28 contempla una lista de los supuestos de mayor riesgo en el tratamiento de datos personales, que deben considerarse por parte del responsable y encargado del tratamiento[508]. Corresponde al responsable del tratamiento evaluar y analizar en todo momento y para todo el ciclo de vida de duración de los datos personales el riesgo[509] que pueda derivarse, y ser capaz de demostrar el cumplimiento de la normativa sobre protección de datos frente a los interesados y las autoridades de supervisión.

El nuevo Reglamento contempla estos principios de la protección de datos desde el diseño y por defecto (*Privacy by Design y Privacy by Default*) como la adaptación al ámbito europeo[510] de un sistema de protección de datos derivado de un entorno masivo de la utilización de Internet y de las nuevas tecnologías, partiendo de la idea de la aplicación del principio de precaución, mediante el desarrollo de un análisis de riesgos preventivo,

---

[507] PIÑAR MAÑAS, J.L., *Reglamento General de Protección de Datos*…, *op.cit*., p. 16.

[508] Art. 28 LOPDGDD:
"a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.
b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.
c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.
d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.
e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.
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.
g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.
h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación".

[509] Para el GT29, el riesgo supone "un escenario que describe un evento y sus consecuencias, estimado en términos de impacto y probabilidad".

[510] Recordemos que el *Privacy by Design* fue desarrollo en Canadá en 1990, apareciendo por primera vez en un informe en 1995. En 2010 se adopta en el seno de la Conferencia Anual sobre protección de datos y Autoridades de protección de la vida privada, una Resolución por todas las autoridades de protección de datos a nivel mundial sobre este principio sobre la idea básica de que la privacidad esté integrada directamente en todo el sistema tecnológico, así como en todo el proceso de tratamiento de datos personales.

de cuyos resultados y de los diversos aspectos derivados del tratamiento, dependerá la aplicación de estos principios.

Así, la protección de datos desde el diseño[511] se basa, como decíamos, en una filosofía preventiva de anticipación y evaluación previa a los posibles efectos que puedan producirse, en la que la protección de la privacidad se mantenga en todo el ciclo de vida de los datos personales, integrándose en la gestión de los sistemas y tecnologías utilizados.

Por parte de los responsables del tratamiento y los productores de servicios, aplicaciones y productos deberán llevar a cabo las medidas previstas en el artículo 21, como la seudonimización y minimización; de forma que la acreditación del cumplimiento de estas medidas podrá acreditarse en base a la certificación prevista en el art. 42 del RGPD.

En relación con la situación de pandemia por el Covid-19, se ha planteado que si el Real Decreto 463/2020, que establece la declaración del estado de alarma, al suspenderse e interrumpirse términos y plazos administrativos, ello conllevaba la suspensión de la obligación de los responsables de notificar las quiebras de seguridad. Por ello, a través de un comunicado de la AEPD se ha señalado que se mantienen "(…) *las obligaciones impuestas en el RGPD relativas a la notificación de brechas de seguridad de datos personales, así como las obligaciones de comunicar a los interesados en caso de que estas entrañen un alto riesgo para los derechos y libertades de las personas físicas* (…)[512].

[511] Art. 25 RGPD.1:
"Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, 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".

[512] AEPD, Comunicación de 2 de abril de 2020.

4.5. SEUDONIMIZACIÓN Y ANONIMIZACIÓN COMO TÉCNICAS DE SEGURIDAD DE LOS DATOS SANITARIOS

En el apartado 1.3, con relación a la investigación biomédica, hemos analizado la seudonimización y la anonimización como técnicas para evitar la identificación del titular de los datos incursos en un proyecto de investigación. Así, la seudonimización, además de una medida se seguridad de los datos, consiste en la anonimización de forma parcial de los mismos; de forma que ya no pueden atribuirse a un interesado sin utilizar información adicional (que figure por separado y sujeta a medidas de seguridad).

Así, los datos resultantes del proceso de tratamiento de seudonimización se consideran datos personales, excepto que esté definido de forma concreta y vinculante un concepto de "datos seudonimizados" que sea diferente del propio de datos personales. Si mediante una información adicional se completan los datos que han sido previamente seudonimizados permitiendo ser atribuidos a una persona física, debe considerarse como persona física identificable y, por tanto, sujeta a protección de datos.

El RGPD es partidario de utilizar la seudonimización como medida de seguridad de los datos, a través del oscurecimiento de los datos, cuya información se relaciona con identificadores artificiales; permitiendo así "(…) *poder reducir el riesgo asociado a la gestión de datos y ayudar a los responsables y encargados del tratamiento a cumplir con sus obligaciones de protección de datos* (…)"[513]; sin que ello suponga excluir cualquier otra medida, como el cifrado de datos en ocasiones concretas, como medida que "(…) *hace ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos* (…)"[514].

Pueden considerarse tres clases de cifrado:

a) Cifrado o encriptación, en la que la información resulta transformada de forma que sólo el emisor y el receptor pueden entenderla.

[513] Considerando 28 RGPD.
[514] Art. 34.3 RGPD.

b) Cifrado privado, es el asociado a la firma digital. Aquí también se encripta la información que puede ser entendida por cualquier persona que la reciba, aunque se oculta el emisor de la información.

c) Cifrado público, en el que la información se encripta de forma que sólo el destinatario concreto pueda recibirla correctamente.

A diferencia del cifrado, la seudonimización permite sólo el acceso de los datos no encubiertos, mientras los datos cifrados permiten a quien disponga de autorización a acceder a la información completa. Ambos pueden llevarse a cabo simultáneamente o bien por separado.

De esta forma, siguiendo a *Cavoukian*[515], para los objetivos de reducir al máximo la materialización de los riesgos que puedan producirse, es necesario que se cumplan los "siete principios fundacionales" de este principio de *Privacy by Design* :

"a) Proactivo, no reactivo;

b) Preventivo no correctivo;

c) Privacidad como la configurada predeterminada;

d) Privacidad incrustada en el diseño;

e) Funcionalidad total –"todos ganan", no "si alguien gana, otro pierde";

f) Seguridad extremo-a-extremo-protección de ciclo de vida completo;

g) Visibilidad y transparencia-mantenerlo abierto;

h) Respeto por la privacidad de los usuarios-mantener un enfoque centrado en el usuario[516]".

[515] CAVOUKIAN, Ann, "*Privacy by Design, The 7 Foundational Principles*", Agosto 2009. Accesible en: www.ipc.on.ca.

[516] DUASO CALÉS, R., "Los principios de protección de datos desde el diseño y protección de datos por defecto" en "Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad", en *Reglamento General de Protección de Datos…, op.cit.*, pp. 296 y ss.

La protección de datos por defecto (*Privacy by Default)*[517], parte de que, al existir una protección de la intimidad previamente predeterminada (protección de datos desde el diseño), por sí misma garantiza la protección de toda la información de carácter personal, aunque por parte de los titulares de los datos no lleven a cabo ningún tipo de acción protectora de sus datos. CAVOUKIAN[518], se refiere a los tres ámbitos en los que actúa este principio: en los sistemas de tecnologías de la información y de la comunicación, en los modelos y prácticas de negocios y en el diseño e infraestructuras en red.

Respeto de los datos anónimos o disociados, se trataría de información que, tanto inicialmente (anónimos) como después del tratamiento (disociados) se convierte en anónima que no se relaciona con una persona física identificada o identificable; quedando al margen de la normativa sobre protección de datos. Así, el proceso de anominación persigue la eliminación de todos elementos que puedan identificar o hacer identificable a una persona, debiendo garantizar que cualquier operación o tratamiento que se realice después de la anonimización no provoca una distorsión de los datos reales.

Por tanto, la anonimización difiere de la seudonimización en que en ésta se suprime la vinculación de los datos con su titular, lo que no significa que los datos se hayan convertido en anónimos, por cuanto a través de una información adicional se pueden atribuir a una persona; por lo que puede identificarse a una persona, aunque de forma indirecta, por lo que se someten a la normativa de protección de datos.

La anonimización de datos como forma de eliminar las posibilidades de identificar a una persona, supone una técnica muy importante[519] en la época actual al permitir el tratamiento y explotación de elevados volúmenes de información; aunque se encuentra amenazada por la propia tecnología que la aplica, haciendo muy difícil conseguir el anonimato absoluto de los datos, aunque si mayores garantías de la privacidad de las

[517] Art. 25.2 RGPD:
"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar 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. 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".

[518] CAVOUKIAN, *Op.cit*.

[519] La AEPD considera que el desarrollo de técnicas de anonimización de datos es fundamental para garantizar la protección de datos personales en el desarrollo de estudios e investigaciones de interés social, científico y económico. "Orientaciones y garantías en los procedimientos de anonimización de datos personales", 11 de octubre de 2016.

personas, siendo necesario que se garantice la irreversibilidad del proceso de anonimización. Así, el riesgo de reidentificación de personas con datos anonimizados está implícito en los tratamientos anonimizados; incrementándose con el paso del tiempo, por lo que debe considerarse su valoración periódica por el responsable del tratamiento.

Partiendo de que, la cadena de identificación de una persona está compuesta de microdatos, que permiten la identificación directa de una persona, y de datos de identificación indirecta, que son aquellos obtenidos de forma relacionada o cruzada con distintas fuentes de información, siguiendo el documento de la AEPD, podemos señalar los siguientes principios a considerar en el proceso de anonimización[520]:

a) Principio proactivo, por el que el principal objetivo perseguido debe ser proteger la privacidad, de forma que su gestión sea proactiva y no reactiva.

b) Principio de privacidad por defecto, desde el inicio se garantice la confidencialidad de los interesados considerando el grado de detalle (escala cuantitativa) que deben tener los datos anonimizados.

c) Principio de privacidad objetiva, en el que tras la evaluación de impacto existirá un riesgo residual de reidentificación que será asumido por el responsable del tratamiento como aceptable y a considerar en el proceso de anonimización.

d) Principio de plena funcionalidad, desde el inicio del sistema de información, se garantizará la utilidad de los datos anonimizados, de forma que no distorsionen a los no anonimizados.

e) Las medidas que garanticen la privacidad de los interesados se aplicarán por todo el ciclo de vida completo de tratamiento de la información, además de la formación e información al personal incurso en el proceso de anonimización y de explotación de la información anonimizada.

[520] AEPD, "Orientaciones y garantías en los procedimientos de anonimizacción de datos personales", 11 de octubre de 2016.

El RGPD, se refiere al empleo de éstas técnicas, en el ámbito del tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos; señalando que este tratamiento deberá realizarse "(…) *cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos(…)*[521]*"*.

5. PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA ASISTENCIA SANITARIA TRANSFRONTERIZA

5.1. TRANSFERENCIAS INTERNACIONALES DE DATOS

Con el aumento del comercio internacional y el desarrollo de las TICs, que han hecho desaparecer las barreras de tiempo y espacio, se ha generado que la transmisión de datos se dé de manera casi inmediata a cualquier parte del mundo, por lo que es indudable que el flujo de datos transfronterizos ha aumentado exponencialmente en los últimos años. Esto ha obligado a muchos países a regular la Transferencia Internacional de Datos. En la actualidad, es sumamente común que una información sea recogida en un lugar, almacenada en otro y se manipulada en un tercer Estado destino a los dos anteriores[522].

La transmisión internacional de datos trae aparejado una serie de riesgos, principalmente en lo relacionado al derecho de la autodeterminación informativa. En primer lugar, en lo que refiere a la pérdida o alteración de los mismos, o que éstos lleguen a manos de terceros y sean usados sin su consentimiento. En segundo lugar, podrían llegar a un Estado en el que el derecho de autodeterminación informativa no se encuentre garantizado. El exceder las fronteras del Estado provoca que la protección sea difícil del controlar, generar riesgos de seguridad nacional, como por ejemplo en la lucha contra el terrorismo[523]. Por tanto, es

[521] Considerando 156 RGPD.

[522] ANCOS FRANCO, H, "La regulación de las transferencias internacionales de datos como barrera al comercio internacional: de la Directiva 95/46 a los acuerdos UE-terceros estados*", Revista de Derecho Comunitario Europeo*, nº 6, 1999, pp. 497-498.

[523] Revista de Administración Pública, nº. 186, Madrid, septiembre-diciembre, 2011, pp. 330-332.

necesario establecer una regulación que asegure un equilibrio entre la necesidad de la transmisión de datos ente países y la protección de la autodeterminación informativa.

La normativa de la Unión Europea en materia de protección de datos es en la actualidad la más exigente. Sin embargo, existen muchos países que han regulado la materia de manera también muy rigurosa, alcanzando los niveles de adecuación exigidos por la Unión Europeo, así como una gran cantidad de Estados que, si bien han regulado la materia, existen grandes deficiencias en el control y garantías para hacer efectivos los derechos fundamentales de los interesados. Por último, existe un gran número de países que aún no han regulado la materia.

La regulación poco exigente, o la inexistencia de la misma, pueden conducir a que la protección procurada por la Unión se disipe cuando los datos se encuentren localizados en Estados sin protección o con niveles inferiores a los regulados por la Unión, por lo que para evitar que se vulneren los derechos de los interesados, se ha regulado detenidamente las transferencias internacionales de datos.

Partiendo de la Directiva 95/46, ésta basaba las transferencias que sólo podrían ser posibles si el país tercero garantiza un nivel de protección adecuado (art. 25.1); ya que, de no ser así estaríamos ante transferencias prohibidas, dejando a salvo las excepciones contenidas en el art. 26. Modelo, que se altera por el RGPD, por lo que, "pueden realizarse transferencias internacionales a terceros países u organizaciones internacionales cuando se basen en una decisión de adecuación, en garantías adecuadas, en alguna de las excepciones del art. 49"[524]

La transferencia internacional de datos se encuentra regulada en el Capítulo V el RGDP, considerándose como tales aquellas en las que el traspaso de los datos personales se da a un encargado o responsable de un Estado u organización internacional externos a la Unión Europea. Cabe aclarar, que, si bien este marco jurídico ha sido establecido por el Parlamento Europeo y por el Consejo de la Unión Europea, El Espacio Económico Europeo ha incorporado el 6 de julio de 201 8, el RGPD al Acuerdo sobre el Espacio Económico Europeo, a través de una decisión del Comité Mixto del Espacio Económico Europeo, que entró en vigor el 20 de julio de 2018. Esencialmente, la disposición

[524] PIÑAR MAÑAS, J.L., "Transferencias internacionales de datos personales a terceros países u organizaciones internacionales", en *Reglamento General de protección de datos*…, *op.cit*., pp. 433-434.

mencionada del Espacio Económico Europeo implica que el RGPD se aplique directamente a Islandia, Noruega y Liechtenstein.

La finalidad del RGDP, como hemos visto a lo largo del presente estudio, es la garantía de los derechos de los interesados sobre el tratamiento de sus datos personales, y se le otorga a la Comisión Europea la tarea de velar por que el tratamiento de los datos observe las garantías exigidas para asegurar la privacidad y que no sea vulnerado ningún derecho fundamental asociado al tratamiento de datos y a su vez, lograr un equilibrio ente la necesidad del flujo transfronterizo y la protección del derecho de autodeterminación informativa[525].

Al amparo del RGDP, la transferencia internacional de datos se considera cuando la misma se da entre un Estado miembro de la Unión Europea o del Espacio Económico Europeo con un país que no pertenece al mismo. En otras palabras, cuando la transferencia se da entre los Estados del bloque no es considerada, a los efectos del Reglamento y de las Directivas respectivas como una transferencia internacional. El RGDP reconoce tres supuestos de transmisión de datos, la cesión, el acceso a los mismos por cuenta de terceros y el movimiento internacional de éstos.

En materia de transferencia internacional de datos, será la Comisión Europea, quien estudie y analice si el Estado receptor de los datos cumple con las garantías mínimas exigidas, en cuyo caso emitirá una declaración de adecuación.

Si bien el tema será desarrollado más adelante, es preciso aclarar que existen tres circunstancias disímiles y cada una con un régimen diferente, según el nivel de adecuación de las normas internas de los Estados y de las organizaciones no comprendidos en el RGDP a éste. En primer lugar, se encuentran los países y organizaciones que cuentan con el nivel adecuado de protección y que cuentan con la Decisión de Adecuación de la Comisión Europea y por tanto no son considerados como tratamiento internacional por lo que no necesitan autorización, en segundo lugar, aquellos países y organizaciones que si bien cuentan con una regulación y un nivel de control acorde al exigido, aún no cuentan con la Decisión de Adecuación y por último, aquellos

[525] Para más información sobre la transferencia internacional de datos sanitarios, vide ABERASTURI GORRIÑO, U.,"Movimiento internacional de datos: especial referencia a la transferencia internacional de datos sanitarios*"*, *Revista de Administración Pública* núm. 186, Madrid, septiembre-diciembre 2011, pág. 330.

países que o bien la regulación no es lo suficientemente garantista o ni siquiera cuentan con regulación en la materia.

Ahora bien, antes de ahondar en los pormenores de los mecanismos para cada una de estas circunstancias, resulta preciso dar una definición clara de lo que significa la transferencia internacional de datos.

Antes de la entrada en vigor del RGDP, la Instrucción de la AEDP establecía "*se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español*". Por su parte, el RDLOPD establecía que la transferencia de datos será aquel "*tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español*[526]", mientras, el RGDP establece en el Capítulo V como "*Transferencias de datos personales a terceros países u organizaciones internacionales"* que la transferencia internacional de datos se da cuando el estado receptor no pertenece al Espacio común[527]. Al referirse a terceros países queda claro que la transferencia entre países del bloque, no serán considerados como transferencia internacional. No obstante, los conceptos cesión y acceso a los datos por cuenta de terceros países, es susceptible a distintas interpretaciones, pudiendo llegar a ser considerado que estos supuestos no constituyen una transmisión de datos, sino que son simplemente, como lo dicen sus nombres una cesión o un permiso de acceso[528].

Por último, es necesario tener en cuenta que, en el entendido de que la transmisión de datos se da entre responsable o encargado designado a otro responsable o encargado del tratamiento de los datos de tercer país u organización internacional, ha sido cuestionado por varios órganos judiciales si cuando esa transmisión se da directamente por el

[526] Art. 5 s) Real Decreto 1720/2007, de 21 de diciembre.

[527] Art. 44. RGPD:

"Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado".

[528] ABERASTURI GORRIÑO A., *op.cit.*, p. 335

interesado, no por un responsable de tratamiento, se configura o no una transmisión internacional de datos, sujeta al RGDP.[529]

En definitiva, podríamos aseverar que existe transferencia internacional de datos cuando los datos y el tratamiento de éstos sale del ámbito de control de la Unión Europea pera ser tratados en un tercer país u organización internacional. Para la AEPD las transferencias internacionales de datos "suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega)"[530].

En lo referente al mecanismo de legitimación para la transferencia internacional, como hemos mencionado, es la Comisión Europea la encargada de velar por el cumplimiento y es quien declara las Decisiones de Adecuación y otorga las autorizaciones para la transmisión con los países que no cuenten con esta.

Para evaluar el nivel de protección de los terceros países u organizaciones internacionales deberán atenderse los siguientes aspectos:

- Que exista en dichos países un Estado de Derecho, un verdadero respeto a los Derechos Humanos, que se encuentren garantizadas las libertades fundamentales, tanto en lo que refiere a los datos personales, así como en materia de seguridad nacional entre otros.
- Que exista en el tercer país a evaluar, una autoridad de control independiente.
- Los compromisos internacionales asumidos por el Estado en cuestión u organización en lo que refiere a la protección de datos personales.

Respecto al contenido se deberá estudiar detenidamente, que dentro de las normas sobre la transferencia internacional de datos se encuentre regulado de manera clara y precisa: las limitaciones sobre el objetivo del tratamiento, la calidad de los datos, el derecho de acceso, de oposición y de rectificación por el interesado, las garantías sobre la

[529] *Ibid.*, pág. 336.
[530] AEPD, Transferencias internacionales, 29 de julio de 2020.

transparencia y las medidas de seguridad para garantizar la efectiva protección de los datos.

En lo que se refiere a los mecanismos para garantizar la efectiva protección de los datos, se deberá analizar: las responsabilidades establecidas respecto a quienes traten los datos, que existan sanciones significativas que promuevan el cumplimiento de las normas de protección, que existan autoridades de control, que estén previstos y en debido funcionamiento los medios adecuados para brindar apoyo y asistencia para hacer efectivo el ejercicio de sus derechos fundamentales y, por último, que se encuentren adecuadamente reguladas y funcionando las vías apropiadas, para quienes pudieran ser perjudicados por el tratamiento de sus datos en el incumplimiento de las normas de protección.

A partir del artículo 45 del RGDP, se regulan todas las situaciones en los que se podrán realizar las transferencias internacionales de datos, sin necesidad de una autorización específica. Para que esto suceda, deben cumplirse alguno de los siguientes supuestos: o bien que el destinatario se encuentre en un país u organización internacional., en el que la Comisión Europea haya declarado previamente que cuenta con un nivel de protección adecuado; en caso de no existir decisión de adecuación, si el receptor ofrece las garantías necesarias; y a falta de las dos anteriores si cumple con las condiciones establecidas en el Reglamento.

Como hemos visto, la Comisión Europea será quien decida si un Estado cuenta con la adecuada protección para ser considerado seguro. El reconocimiento de la Comisión Europea, a través de la Decisión de Adecuación, implicará que no sea necesaria ninguna autorización o trámite especial a la hora de transferir datos con aquellos países que hayan sido declarados seguros. Es de destacar en este sentido, por su mayor impacto el "*Escudo de Protección Privacy Shield*" entre la Unión Europea y los Estados Unidos de América[531].

Por otro lado, cuando la transmisión se da a un país u organización que no cuenten con la decisión de adecuación, el RGDP permite al responsable o encargado realizar las transferencias internacionales sin autorización previa, siempre que adopte las garantías

[531] Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.

adecuadas. Estas garantías podrán establecerse por medio de "*a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados*.[532]"

Cuando no existe Decisión de adecuación, ni tampoco existen las garantías adecuadas sólo se podrá trasferir información, con la autorización previa de la autoridad de control ante quien deberá probarse que se cumplen con las condiciones establecidas en el artículo 49 del RGDP, como, por ejemplo: que exista el consentimiento explícito de los interesados después de ser notificado sobre los posibles riesgos, o que la transmisión sea necesaria para la celebración, la ejecución o el cumplimiento de un contrato, o para hacer efectiva una medida precontractual.

La actual regulación contenida en el RGPD ha traído consigo considerables novedades sobre dichas transferencias; una de ellas reside en que el exportador de los datos puede, ahora, ser a su vez el responsable y encargado del tratamiento, pero deberá tomar las medidas necesarias para garantizar, entre otros aspectos, la seguridad en la transmisión[533], de ahí, que ahora no resulta aplicable la condición que algunos Estados Miembros habían impuesto para este tipo de operación y que consistía en que el exportador debía ser siempre el responsable del tratamiento. Este Reglamento también condiciona que casi la totalidad de tratamientos de datos personales, incluidas las transferencias de datos internacionales, estarán sujetos a este instrumento abarcando las relacionadas a fines comerciales, así como con el cumplimiento de la ley o tratados internacionales.

Tal como señala CORDERO[534], los responsables y encargados del tratamiento podrán realizar transferencias internacionales de datos sin que medie, necesidad de una

[532] Art. 46 RGPD.

[533] Considerandos 11 y 118 del RGPD.

[534] "En términos generales, desde la perspectiva española, puede referirse un cambio relevante respecto de la tramitación administrativa que estas operaciones requerían con la Directiva-LOPD, esto es, solicitud de previa autorización administrativa (artículo 33.1 LOPD) –y aprobación de la AEPD– salvo las excepciones del artículo 34 LOPD. El Reglamento en este sentido da un giro total dejando la autorización administrativa a casos realmente excepcionales, de tal manera que la autorización administrativa pasa de ser la norma general a ser una excepción muy concreta (en este sentido se recoge en el art. 42 de la nueva LOPD de 2018)". CORDERO, C., "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: Especial referencia al caso estadounidense. Especial referencia al "caso

autorización de la AEPD, en cuanto el tratamiento de datos observe lo dispuesto en el Reglamento y se cumpla alguno de los supuestos siguientes: 1. Transferencias internacionales de datos basadas en una decisión de adecuación (artículo 45 RGPD). 2. Transferencias mediante garantías adecuadas (artículo 46 RGPD). 3 *"Binding corporate rules"* (artículo 47 RGPD) o 4. Se cumpla con alguna de las excepciones previstas.

Para el primer supuesto, el artículo 45 del Reglamento señala que se podrá realizar una transferencia de datos personales a un tercer país u organización internacional, sin ninguna autorización administrativa previa "*cuando la Comisión haya decidido que el tercer país, un territorio o varios sectores específicos de ese tercer país (…) garantizan un nivel de protección adecuado*"[535].

Durante el año 2011 se tramitaron 175 autorizaciones a empresas para realizar transferencias internacionales de datos a países con un nivel no equiparable de protección, y en las que *"El nivel de exigencia es tan alto que produce un efecto disuasorio cuya consecuencia es que el responsable renuncia antes de haberse planteado siquiera empezar con la tramitación"*[536].

Por su parte, en el segundo supuesto, el Reglamento establece en su artículo 46, que será necesaria la presentación de garantías cuando se desee efectuar transferencias a países u

estadounidense y la Cloud Act."., *Revista Española de Derecho Europeo* num.70/2019, parte Estudios, 49.107.

[535] Artículo 45 RGPD.

A la fecha, los países considerados como adecuados de acuerdo a la Comisión Europea son los siguientes:

PAÍS	**AUTORIZACIÓN**
Andorra	Decisión 2010/625/UE de la Comisión, de 19 de octubre 2010.
Argentina	Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.
Canadá	Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001.
Estados Unidos	Solo si la entidad está adherida al Escudo de Privacidad o *"Privacy Shield"*[535].
Guernesey	Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
Isla de Man	Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
Islas Feroe	Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
Israel	Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
Jersey	Decisión 2008/393/CE de la Comisión, de 8 de mayo de 2008.
Nueva Zelanda	Decisión 2013/65/UE de la Comisión, de 21 de agosto de 2012.
Suiza	Decisión 2000/518/CE de la Comisión, de 26 de julio de 2010.
Uruguay	Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
Japón	Decisión de 23 de enero de 2019.

[536] SALDAÑA, Jordi, *Actualidad Jurídica Aranzadi num.836/2012,* Editorial Aranzadi, Cizur Menor. *2012.*

organizaciones no aprobadas por la Comisión, a saber: Un documento con vinculación jurídica exigible entre organismos públicos o autoridades; código de conducta o mecanismos de certificación donde el responsable de datos se comprometa a garantizar el respeto a los derechos protegidos así como la aplicación de las medidas necesarias para su indemnidad, normas corporativas que revistan carácter vinculante y/o la utilización de las llamadas "cláusulas tipo" en materia de protección de datos adoptadas por la Comisión o adoptadas por la AEPD. Además, dicho artículo prevé que, en los casos indicados reglamentariamente, se entenderá que la transferencia tiene garantías adecuadas como las que se realizarían dentro de territorio común.

Sobre lo relacionado con las "*Binding corporate rules*" (BCR) o normas corporativas vinculantes, son, como señala la AEPD[537] "l*as 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*".

De acuerdo con el GT29[538], las BCR se corresponden a aquellas políticas de protección de datos que se aplican dentro de un grupo empresarial[539] o unión de empresas dedicadas a una actividad económica conjunta, por el encargado o responsable de tratamiento que se encuentre en un Estado miembro sobre las transferencias o sobre un conjunto de transferencias de datos personales a un encargado o responsable en uno o varios países fuera de la unión.

Sobre estas normas, el artículo 47 RGPD establece que la autoridad de control aprobará normas corporativas de carácter vinculante a las que se podrán unir los grupos de empresas, permitiendo salvaguardar la transferencia de datos, de conformidad con el mecanismo de coherencia establecido en el artículo 63 del Reglamento[540]. Es importante destacar que es la primera vez que, en materia de protección de datos, las *BCR* tienen

[537] AEPD, Transferencias internacionales, 29 de julio de 2020.
[538] GT 29, "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", 29 de noviembre de 2017.
[539] Para la AEPD, documento de 29 de julio de 2020, serían aquellos "*constituidos por una empresa que ejerce el control y sus empresas controladas*".
[540] Artículo 67 RGPD.

rango legal[541]; las mismas se consideran jurídicamente vinculantes y deben ser cumplidas por todos los miembros del grupo empresarial o unión de empresas. Además, deben conferir a los interesados derechos exigibles y, por último, deben cumplir unas formalidades tasadas en el artículo 47.2 del RGPD[542].

Ahora bien, en caso de falta de decisión de adecuación y de garantías adecuadas solamente se podrán realizar las transferencias si se presenta alguna de las situaciones descritas en el artículo 49 del RGPD, como por ejemplo el consentimiento explícito del interesado, la transferencia sea necesaria por razones vitales de interés público; debido a la formulación, el ejercicio o la defensa de reclamos; cuando el interesado se encuentre incapacitado legal o físicamente para otorgar tu consentimiento y/o la transmisión se realice desde algún registro público que en observancia al Derecho de la Unión se encuentre abierto a consulta pública y tenga como finalidad proveer información al público siempre que se cumplan los supuestos que establece el Derecho de la Unión o de los Estados miembros para dicha consulta.

5.2. PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA ASISTENCIA SANITARIA TRANSFRONTERIZA

5.2.1. ASISTENCIA SANITARIA Y PROTECCIÓN DE DATOS

El art. 35 de la CDFUE establece el derecho de las personas a la prevención sanitaria, así como a beneficiarse de la atención sanitaria conforme a la legislación nacional, garantizándose un alto nivel de protección de la salud humana, lo que se relaciona con lo dispuesto en el art. 20 del TFUE sobre los principios de libertad de circulación y ciudadanía europea; lo que, a juicio del TJUE, incluye todos los tipos de atención médica, aunque sin reconocer su naturaleza específica[543].

No obstante, hay que resaltar que el verdadero impulso de la asistencia sanitaria transfronteriza ha venido de la mano de la jurisprudencia del TJUE, a través de la relación

[541] El GT ya las adoptó tiempo atrás y ha ido actualizando sus posicionamientos.
[542] La BCR aprobada por la AEPD hasta la fecha sería:
TI-00001-2020-Resolución de Autorización GRUPO FUJIKURA AUTOMOTIVE EUROPE – 11-03-2020.
[543] STJUE de 15 de julio de 2010, asunto C-345/09.

de las libertades de circulación y establecimiento y prestación de servicios con los Reglamentos de coordinación en materia de seguridad social[544].

Así, esta jurisprudencia, suponía reconocer una especie de derecho a la "libre circulación de pacientes", que devino en el llamado "turismo sanitario", caracterizado por los problemas financieros que causa al Servicio de Salud receptor[545].

Ello, sirvió de base para dictar la Directiva 2011/24 relativa a los Derechos de los Pacientes en la Atención Sanitaria Transfronteriza; la cual contiene entre sus objetivos generales": a) fomentar el establecimiento de procedimientos para facilitar el acceso a la atención sanitaria transfronteriza segura y de alta calidad, asegurando la movilidad de pacientes de acuerdo con los principios del TJUE; y b) promover la cooperación en la atención sanitaria entre los Estados miembros"[546].

El contenido de la Directiva 211/24/UE se aplica a los denominados "registros médicos" o Historia clínica, que se definen 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*" (art. 3.m).

Como resultado de la trasposición de la misma ha surgido el Real Decreto 81/2014, de 7 de enero, por el que se establecen normas para garantizar la asistencia sanitaria

544 Reglamentos 883/2004 y 987/2009.

545 GARCÍA MURCIA, J.; RODRÍGUEZ CARDO, I.A., "Asistencia sanitaria transfronteriza en el ámbito de la unión europea: de la seguridad social de trabajadores migrantes a una regulación específica", *Foro Nueva Época*, vol.17, nº 1, 2014, pp. 309-329.

546 Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a los Derechos de los Pacientes en la Atención Sanitaria Transfronteriza. El objetivo de la presente Directiva es establecer unas reglas para facilitar el acceso a una asistencia sanitaria transfronteriza segura y de elevada calidad en la Unión, así como garantizar la movilidad de los pacientes de conformidad con los principios establecidos por el Tribunal de Justicia y promover la cooperación en materia de asistencia sanitaria entre los Estados miembros, respetando plenamente, al mismo tiempo, las responsabilidades de los Estados miembros en lo tocante a la determinación de las prestaciones de seguridad social que estén relacionadas con la salud y a la organización y la prestación de asistencia sanitaria y atención médica, y de otras prestaciones de la seguridad social, en especial, en caso de enfermedad (Considerando 10 de la Directiva). La Directiva ha sido completada por la Decisión de Ejecución de la Comisión, de 10 de marzo de 2014, por la que se fijan los criterios para la creación y evaluación de las redes europeas de referencia y de sus miembros, y se facilita el intercambio de información y conocimientos en materia de creación y evaluación de tales redes y la Decisión Delegada de la Comisión, de 10 de marzo de 2014, por la que se establecen los criterios y las condiciones que las redes europeas de referencia y los prestadores de asistencia sanitaria, que deseen ingresar en las redes europeas de referencia, deben cumplir, en síntesis, las condiciones de organización, evaluación y funcionamiento de las redes europeas de referencia previstas en dicha Directiva, así como al establecimiento de las condiciones que deben cumplimentar los prestadores de asistencia

transfronteriza, y por el que se modifica el Real Decreto 1718/2010, de 17 de diciembre sobre receta médica y órdenes de dispensación.

No obstante, no debe olvidarse que, partiendo del principio de no discriminación por razón de nacionalidad, el objeto de la Directiva no es garantizar los derechos de los pacientes en cualquier situación y ante toda clase de asistencia sanitaria transfronteriza, sino en relación a la cubierta por los Reglamentos de coordinación en materia de seguridad social[547]. De forma, que la asistencia sanitaria transfronteriza se realizará de conformidad con "(…) *el derecho fundamental a la intimidad con respecto al tratamiento de los datos personales quede protegido de conformidad con las medidas nacionales de aplicación de las disposiciones de la Unión relativas a la protección de los datos personales*" (art. 4.1.e).

La garantía de la continuidad asistencial se realizará de forma que "(…) *los pacientes que hayan recibido tratamiento tengan derecho a obtener en papel o en forma electrónica la historia clínica de dicho tratamiento y como mínimo una copia del mismo, de conformidad con las medidas nacionales de aplicación de las disposiciones de la Unión de protección de los datos personales*" (art. 4.1.f); o bien "(…)*puedan tener acceso remoto, o al menos dispongan de una copia de su historia clínica* (…)(art. 5.d).

Por su parte, el RD 81/2014, se hace eco de estos postulados de la Directiva, y en relación con la asistencia sanitaria prestada en otro Estado miembro a pacientes cuyo Estado de afiliación es España, establece que se garantizará:

"*a) La disponibilidad de una copia, en el soporte adecuado, de los informes clínicos, y de los resultados de pruebas diagnósticas y/o procedimientos terapéuticos, difundiéndose el procedimiento para su acceso.*

b) Desde las administraciones públicas se promoverá el acceso electrónico a la documentación clínica por medio de los sistemas de información dispuestos a tal efecto por el ordenamiento jurídico.

c) La cooperación con otros Estados miembros en el intercambio de la información oportuna que garantice la continuidad asistencial se deberán aplicar los estándares

[547] MERCHÁN MURILLO, A., y TORRALBO CARMONA, A.,"Proyecto EpSOS: una sanidad electrónica transfronteriza en Europa". *Revista General de Derecho Administrativo*, nº 48, mayo 2018.

nacionales, europeos e internacionales de comunicación de la historia clínica electrónica o de sus componentes, con las garantías de seguridad en el tratamiento de datos establecidas en la legislación española en materia sanitaria y de protección de datos de carácter personal"[548].

El proveedor de asistencia sanitaria, además de suministrar al paciente la información contenida en el art. 8, garantizará "(…) *al paciente la disponibilidad de una copia de su historia clínica que permita la continuidad de la prestación de la asistencia de los pacientes atendidos que procedan de otros Estados miembros y que requieran seguimiento dentro del ámbito de la asistencia sanitaria transfronteriza*" (apdo.7).

En el entorno actual de universalidad de datos personales en la sociedad de la información, caracterizado por un uso masivo de herramientas tecnológicas a través de la red (*e-Healt*), resulta trascendental para el propio desarrollo de los sistemas un uso adecuado de los mismos; de forma que resulte compatible la rapidez y el acceso masivo de información con la seguridad con el respeto a la privacidad de los afectados por la información, mediante un tratamiento de datos adaptado al principio de calidad de los datos: adecuado, pertinente y no excesivo en relación con los objetivos perseguidos; los cuales deben ser explícitos, legítimos y determinados en el momento de la obtención de los datos.

Ya hemos visto como la digitalización de la HC incorpora distintos registros electrónicos de salud, que, además de sus enormes ventajas, como una mejor incidencia en el proceso asistencial de los pacientes, o en su prevención o diagnóstico, además de una reducción de costes, supone, por el contrario, importantes riesgos y amenazas en cuanto a la seguridad, privacidad e integridad de los datos sanitarios, latentes en todo momento, y que ponen a prueba la confianza del paciente en el sistema. Así, pese al empleo de la anonimización mediante la supresión de los datos identificativos de los datos de la persona, existe la amenaza de intrusión en la intimidad mediante los llamados ataques de enlace que pueden llegar a eludir el cifrado de datos. Por ello, resulta fundamental crear

[548] Art. 6. Real Decreto 81/2014, de 7 de enero, 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.

un clima de confianza en la utilización de los ciudadanos en los sistemas de salud electrónica nacional e internacional mediante la protección efectiva de los datos sanitarios.

5.2.2. INTEROPERABILIDAD DE LOS SISTEMAS SANITARIOS

La Directiva 81/2014 reconoce la existencia de diferencias regulatorias en los sistemas sanitarios europeos, que incluyen diferentes formatos y estándares tecnológicos, muchas veces incompatibles entre sí, lo que supone obstáculos a la normal asistencia transfronteriza, además de la posibilidad de riesgos para los pacientes. Así, como medida de seguridad debe tenderse a la interoperabilidad de las soluciones tecnológicas de *eHealth*; por cuanto que la ausencia de interoperabilidad de las HCE puede suponer un obstáculo para los propios objetivos de la *eHealth.* Y esta finalidad de homogeneidad en las soluciones tecnológicas debe lograrse:

"(…) *dentro del respeto de las normativas nacionales sobre la prestación de servicios de asistencia sanitaria adoptadas para la protección del paciente, incluida la legislación sobre las farmacias por Internet, en particular las prohibiciones nacionales de venta a distancia de medicamentos dispensados únicamente con receta médica, en tanto en cuanto que sean conformes con la jurisprudencia del Tribunal de Justicia, la Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia (1) y la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior*"[549].

Como instrumentos para conseguir la interoperabilidad de sistemas de las TIC´s se establecen:

[549] Considerando 57 de la Directiva 81/2014, de 7 de enero.

a) Los Puntos de Contacto Nacionales. El RD. 81/2014, establece que será el Ministerio de Sanidad el responsable de la información al ciudadano (art. 7).

b) La Red Europea de Sanidad Electrónica (*eHealth Network*), que, creada por la Directiva 211/24, surge para apoyar y facilitar la cooperación e intercambio de información entre los Estados miembros, que de forma voluntaria pueda conectar a las autoridades nacionales responsables (art. 14.1 de la Directiva).

Su creación permite constituir un espacio europeo de datos sanitarios, bajo la presidencia de Alemania y de la Comisión Europea, que trabaja básicamente sobre el intercambio electrónico de historiales médicos, a través del llamado "proceso de coordinación conjunta". Todo ello, con la finalidad de conseguir un intercambio de registro de pacientes dentro de un "marco común de intercambio de información sobre salud"[550].

Al mismo tiempo, los objetivos de la Red serían[551]:

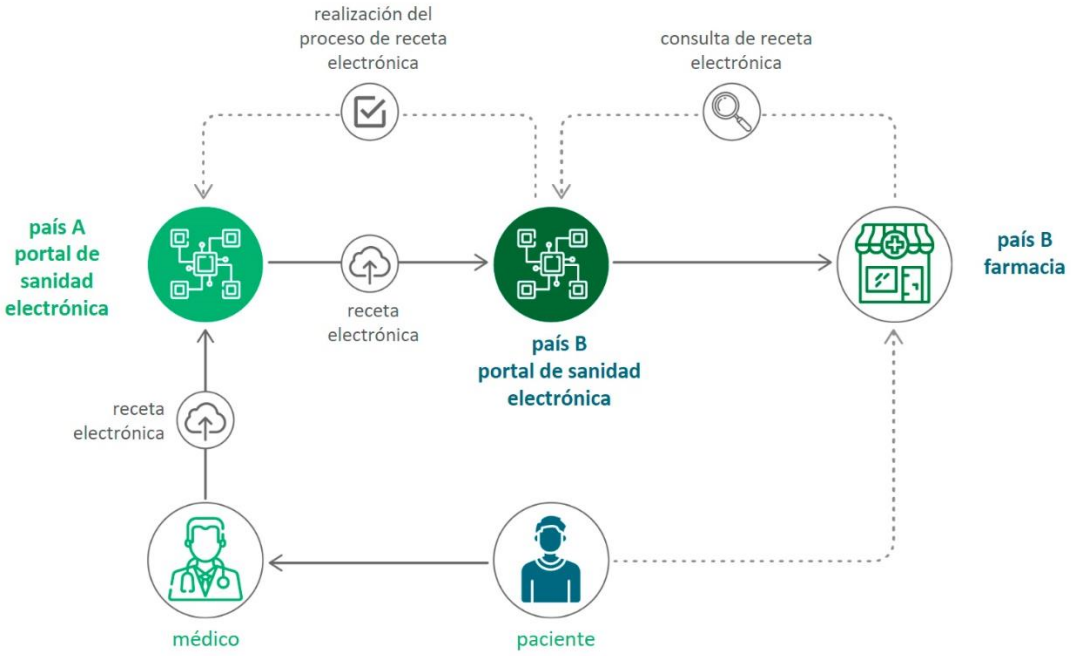
1. Realizar actuaciones tendentes a que los "sistemas y servicios europeos de sanidad electrónica y a aplicaciones interoperables que permitan alcanzar un alto grado de confianza y seguridad, mejorar la continuidad de los cuidados y garantizar el acceso a una asistencia sanitaria segura y de calidad"
2. La elaboración de directrices relativas a "una lista no exhaustiva de datos que deberán incluirse en el historial de los pacientes y podrán ser compartidos por los profesionales sanitarios para propiciar una continuidad en los cuidados y la seguridad de los pacientes a través de las fronteras", además de contener "unos métodos eficaces que permitan utilizar los datos médicos en beneficio de la salud pública y la investigación".
3. "Apoyar a los Estados miembros para que impulsen medidas comunes de identificación y autenticación para facilitar la transferibilidad de los datos en la asistencia sanitaria transfronteriza".

Derivado de la Directiva, se está trabajando a nivel europeo en la receta electrónica interoperable entre Estados, estando previsto que pueda finalizarse en 2021. España está

[550] Redacción Médica, 12 de noviembre de 2019. Accesible en: https://www.redaccionmedica.com/
[551] Art. 14 de la Directiva 211/24/UE, de 9 de marzo de 2011.

siendo de los últimos países en ir incorporando el intercambio de datos clínicos. Será durante el año 2020, que los españoles podrán acceder a sus historias clínicas y a sus recetas desde Austria, Italia, Hungría, Irlanda, Polonia, Alemania y Francia. Así, la Comisión, junto con los Estados miembros, está construyendo una infraestructura voluntaria de servicios digitales de sanidad electrónica (*eHDSI*) para permitir el intercambio de datos sanitarios de pacientes, concretamente recetas electrónicas e historiales de pacientes, más allá de las fronteras nacionales.

En este proyecto participan 22 Estados miembros y su finalidad es conectar sus sistemas de sanidad electrónica a la infraestructura de sanidad electrónica de la UE a través de un portal específico conocido como el punto nacional de contacto para la sanidad electrónica (*PNCeS*)[552]



Procedimiento para el intercambio transfronterizo de recetas electrónicas (Informe 07/19 Tribunal Cuentas Europeo).

[552] Informe 07/2019 del Tribunal de Cuentas de la Unión Europea. Disponible en https://op.europa.eu/webpub/eca/special-reports/cross-border-health-care-7-2019/es/

El proyecto *EpSOS*, forma parte de la estrategia general en *eHealth*, y trata de establecer marcos de interoperabilidad para los sistemas de información, a través del apoyo al desarrollo y utilización de soluciones de sanidad electrónica interoperables, con una especial atención a la aplicación de la telemedicina y la salud móvil (*mHealth*), centrándose en el intercambio de datos de resumen de pacientes y recetas electrónicas entre países europeos"[553].

EpSOS persigue dos objetivos básicos: poder permitir que un paciente en una situación imprevista o no programada que se encuentra fuera de su país de la UE pueda ser atendido por un profesional accediendo al contenido mínimo de datos de salud de su HCR o *Patient Summary;* y que pueda suministrarse a un paciente un medicamento prescrito en otro país, o que la prescripción se realice en el país que no es de su origen y se suministre en el de origen, mediante el acceso a las prescripciones facilitadas por la Receta electrónica.

[553] Proyecto de Salud transfronteriza "EpSOS": http://epSOS.eu

PARTE II

PROTECCIÓN DE DATOS Y LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA SANITARIA

CAPÍTULO I

TRANSPARENCIA EN LA ACTIVIDAD PÚBLICA SANITARIA

1. LA TRANSPARENCIA COMO ELEMENTO ESENCIAL DE PARTICIPACIÓN DE LOS CIUDADANOS EN EL ÁMBITO DE LA SALUD

1.1. LA TRANSPARENCIA PÚBLICA

La sociedad exige cada vez que sus Administraciones públicas sean más transparentes, así como que exista una mayor participación de los ciudadanos en la toma de decisiones públicas; lo que permite una mayor proximidad de los administrados a sus instituciones y un mayor control de sus actividades. Junto a estos principios, el derecho de acceso a la información pública se configura como un elemento vertebrador de la transparencia y la rendición de cuentas, los cuales permiten evaluar el grado de calidad democrática de las instituciones.

En contraste con la regla del carácter secreto de las sesiones de los ayuntamientos del antiguo régimen, el constitucionalismo liberal impulsa la publicidad de las actuaciones parlamentarias y judiciales, durante casi dos siglos, en los cuales fue imposible incluir al poder ejecutivo, debido al enfoque individualista aplicado al principio de legalidad, dejando la iniciativa a la propia actuación de los particulares. El paradigma de la reserva o confidencialidad ha cedido su espacio al de la transparencia pública para reforzar la necesaria legitimación democrática y coadyuvar al respeto de la legalidad por parte de las autoridades y sus agentes

En esta línea, venimos asistiendo, en nuestro país, a un cambio de paradigma en lo que constituye la Administración pública, derivado de las relaciones entre los poderes públicos y el ciudadano, en el que éste exige ante todo servicio público, prestado con honestidad, eficiencia, apertura y responsabilidad; demandando participar y solicitando información adecuada para poder valorar la calidad de ese servicio. Al mismo tiempo, este ciudadano de nuestro tiempo exige un mayor control sobre la actividad política y la gestión de los organismos públicos y de sus recursos, para lo cual resulta imprescindible que la Administración garantice la transparencia administrativa y promueva el acceso a la información pública por medios electrónicos.

El principio de transparencia se recoge en los artículos 1 y 10 del Tratado de la UE, garantizando una mayor participación de los ciudadanos en el proceso de toma de decisiones, así como una mayor legitimidad, eficacia y responsabilidad de la Administración para con los administrados en un sistema democrático[554].

Como consecuencia del avance de la sociedad democrática y tecnológica se aprecia un incremento de la trascendencia que viene a suponer el derecho de acceso a la información pública tanto para para los ciudadanos en general como para los Estados y la propia institución de la Unión Europea; considerándose como un instrumento fundamental dirigido a garantizar la transparencia de la actuación de los poderes públicos y, por tanto, como un elemento de legitimación democrática. Y, así, la transparencia en el funcionamiento de las instituciones del Estado facilita la participación, según ha sido entendido en el Derecho comunitario, al hablar de "apertura" de las instituciones comunitarias que garantizarán una mayor participación de los ciudadanos, al hacerse referencia a que las decisiones serán tomadas de la forma más abierta y próxima a los ciudadanos que sea posible[555].

De esta forma, partiendo del principio constitucional de la participación de los ciudadanos en los asuntos públicos (art. 9.2. C.E.), la transparencia de la actividad pública supone un instrumento de control del ejercicio de la acción pública, y de legitimación del poder

[554] ÁLVAREZ HERNANDO, J., "Tratamiento de datos personales en la Administración Pública", *Practicum Protección de Datos,* Aranzadi, 2014, pp. 23-31.
[555] Art 1º, 2 del Tratado de la Unión Europea, de 7 de febrero de 1992.

político, a través de las distintas vertientes sobre las que la transparencia se manifiesta o incide.

Podemos decir, que los distintos preceptos constitucionales potencian la participación de la sociedad civil, la existencia de una opinión pública activa y la transparencia. Así, la participación directa del ciudadano en los asuntos públicos (art. 23.1.CE), está relacionada íntimamente con el principio democrático (art. 1.1 CE), con la obligación de los poderes públicos de facilitar la participación efectiva de los ciudadanos en la vida política, social, económica y cultural (art. 9.2 CE), y con el art. 105 CE[556], que aborda la participación ciudadana en el procedimiento administrativo y a través de los archivos y registros administrativos.

De esta forma, el art. 105 CE incluye un conjunto de garantías que resultan trascendentales para el funcionamiento de un Estado democrático de Derecho: la primera, que supone que los ciudadanos pueden participar con la Administración en la elaboración de disposiciones de carácter general; la segunda, la obligación de la Administración de canalizar toda su actuación administrativa a través de un procedimiento, como cauce legal de actividad en el que el ciudadano debe ver garantizada la posibilidad de defensa de sus derechos mediante el trámite de audiencia en el mismo; y, por último, el derecho de acceso de los ciudadanos a los archivos y registros administrativos. De esta forma, el principio de participación constituye el fundamento de los apartados a) y c) del art. 105 CE, que se materializa a través de los tres medios de intervención en la actuación administrativa señalados.

El TC reconoce en distintas sentencias que el principio participativo se encuentra reconocido en el art. 105 CE. Así, se ha pronunciado sobre el derecho de participación en la actuación administrativa, como consecuencia de la elaboración de disposiciones de carácter general, señalando:

"El derecho a la participación que se considera vulnerado no es un derecho de participación política incardinable en el art. 23.1 CE. Se trata de una participación en la actuación administrativa, que no es tanto una manifestación del ejercicio de la

[556] Este artículo introduce en un nuestro ordenamiento un principio de publicidad y transparencia en la acción administrativa directamente lanzado contra las restricciones impuestas en el pasado por la Ley de Secretos Oficiales: Fernández Rodríguez, T.R., "La organización territorial del Estado y la Administración Pública en la nueva Constitución", en *Lecturas sobre la Constitución Española* (I), UNED, 1978, p. 369.

soberanía popular, cuanto uno de los cauces de los que en un Estado social deben disponer los ciudadanos (…) para que su voz pueda ser oída en la adopción de decisiones que les afecten (…) Se trata de una participación en la actuación administrativa, de carácter funcional o procedimental, que garantiza tanto la corrección del procedimiento cuanto los derechos e intereses legítimos de los ciudadanos"[557].

Así mismo, en relación con la audiencia de los interesados y de los ciudadanos (art. 105 a) y b)[558]:

> *"(…) Se trata pues, de un principio inherente a una Administración democrática y participativa, dialogante con los ciudadanos, así como de una garantía para el mayor acierto de las decisiones, conectada a otros valores y principios constitucionales, entre los que destacan la justicia y la eficacia real de la actividad administrativa (arts. 1, 31.2 y 103 CE)"*[559].

Cuando hablamos de transparencia, en el sentido de la LTBG y de las leyes autonómicas, podemos referirnos a dos ámbitos diferenciados de la misma: la publicidad activa (transparencia activa) y el derecho de acceso a la información pública (publicidad pasiva). La primera, supone la difusión, por el propio organismo público, de la información que obra en su poder, de forma veraz, actualizada, objetivada, comprensible y gratuita, en los medios (normalmente electrónicos) de acceso universal y gratuito, con las limitaciones derivadas de la protección de datos personales y de otros derechos; todo ello, con la finalidad de los ciudadanos conozcan la información que sea importante para garantizar la transparencia de la actividad pública.

Sin embargo, el derecho de acceso a la información pública se configura como un derecho de cualquier persona a solicitar información en poder de un organismo público, que hayan sido elaborada o adquirida en el ejercicio de sus funciones; estando limitada por los límites previstos en la ley (art. 14 LTBG), y por las causas de no admisión (art. 18.1

[557] STC 119/1995, de 17 de julio.
[558] STC 102/1995, de 26 de junio.
[559] En igual sentido, la STS de 4 de julio de 1987, señala que "el denominador común de los tres supuestos contemplados en el art. 105 CE consiste en la participación ciudadana y en la transparencia de la estructura burocrática".

LTBG), fundamentalmente la existencia en el contenido de la información de datos de carácter personal (en especial de índole sanitario).

En el estado inicial de la epidemia de COVID-19, con la declaración del estado de alarma, por el Real Decreto 463/2020, de 14 de marzo, se declara plenamente operativa la transparencia activa (aunque ya hemos visto que el Portal de transparencia sanitario estaba congelado); mientras la transparencia pasiva quedaba en suspenso, en base a la Disp.Adic.3ª[560].

Para *DEBBASCH*[561], el concepto de transparencia viene a denotar una transformación del concepto de publicidad de la actuación administrativa[562] en un movimiento de transformación de la Administración hacia el exterior, por cuanto la idea de transparencia es más amplia y exigente que la de publicidad. Así, se ha pasado por parte del ciudadano de una idea de consentimiento como forma participativa a otra de necesidad de conocimiento, en la que para que un ciudadano moderno y más informado acepte que se le gobierne previamente tiene que conocer la acción del Estado. Surge así esta moderna idea de conocimiento que identifica a la transparencia formando parte de la tercera generación de los derechos del hombre; por lo que sin ella la Administración carecerá de verdadera legitimación en su actuación.

Resulta conocida la consideración de *DEBBASCH* de la transparencia como una "casa de cristal", en la que interaccionan tres factores en favor del ciudadano: a) el derecho a

[560] Disp.Adic.3ª R.D. 463/2020, de 14 de marzo:
1. "Se suspenden términos y se interrumpen los plazos para la tramitación de los procedimientos de las entidades del sector público. El cómputo de los plazos se reanudará en el momento en que pierda vigencia el presente real decreto o, en su caso, las prórrogas del mismo. La suspensión de términos y la interrupción de plazos se aplicará a todo el sector público definido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

2. No obstante lo anterior, el órgano competente podrá acordar, mediante resolución motivada, las medidas de ordenación e instrucción estrictamente necesarias para evitar perjuicios graves en los derechos e intereses del interesado en el procedimiento, y siempre que éste manifieste su conformidad, o cuando el interesado manifieste su conformidad con que no se suspenda el plazo.
3. La presente disposición no afectará a los procedimientos y resoluciones a los que hace referencia el apartado primero, cuando estos vengan referidos a situaciones estrechamente vinculadas a los hechos justificativos del estado de alarma".

[561] DEBBASCH, C., Introducción, en "La transparence administrative en Europe", Editions du Centre National de la Recherche Scientifique, Paris, 1990, pp. 11 y ss.

[562] Así, RAMS RAMOS, L., *El derecho de acceso a archivos y registros administrativos*, Colección de Derecho Administrativo, (Dir. PIÑAR MAÑAS, J.L.) Madrid, 2008, pp.199-200, señala que no hay más que observar como las primeras sentencias que se refieren al art. 105 CE hablan del principio de publicidad (STS de 6 de octubre de 1979), y sin embargo, posteriormente, se refieren a los principios de transparencia y participación (STS de 4 de julio de 1987, entre otras).

conocer; a saber qué hace la Administración, ya que debe estar al servicio de los ciudadanos; b) del derecho a controlar; ya que si se conoce lo que hace la Administración puede controlarse mejor sus actuaciones en cuanto a su legalidad y oportunidad; y, c) por último, el ciudadano no debe ser un simple espectador ante la Administración, sino que debe poder ser un actor con facultades de actuación. De forma que para la consecución de estos elementos el ciudadano dispone de la participación[563]: en el procedimiento administrativo (acceso y motivación de los actos) y mediante el acceso a la información pública[564].

El sistema de gobierno mediante la democracia parlamentaria tiene como base la confianza del pueblo en las instituciones y sus gobernantes, para lo que es preciso que exista transparencia en la actuación de los poderes públicos; manifestada a través de la información pública y suministro de información, que permite al ciudadano poder participar en los asuntos públicos, a través del acceso a los registros y documentos públicos; con las excepciones derivadas de la normativa comunitaria y las propias relativas al respeto de los derechos fundamentales, en especial los de carácter personal.

Así, dentro de los principios generales de funcionamiento de la Administración en relación con los ciudadanos, se encuentra el de transparencia y participación, recogidos en el art. 3.1.c). de la LRJSP. Para la consecución de una calidad de gobierno mediante una gestión pública imparcial, ética, abierta, eficaz, eficiente y responsable son imprescindibles la transparencia y la participación ciudadana. La transparencia, que se articula sobre la publicidad y el acceso a la información administrativa –básicas en la sociedad de la información en que estamos-, propicia la imparcialidad, la formación de una opinión pública informada y libre y la implicación ciudadana; y la participación social aporta una pluralidad de intereses de todo tipo y refuerza la legitimidad democrática.

Con ello, se trata de profundizar en el valor democrático sustentando, en la dignidad de la persona humana y sus derechos, un nuevo estadio de democracia participativa, complementando la tradicional democracia representativa; lo que, además, permite un

[563] El art. 5.1 de la Ley de Cohesión del Sistema Nacional de Salud contempla la participación de los ciudadanos y profesionales en el Sistema Nacional de Salud.
[564] RAMS RAMOS L., *op.cit.*, pp. 199-200.

control de los ciudadanos sobre la acción de los poderes públicos, coadyuvando en la lucha contra la corrupción.

SANZ SALGUERO, en su estudio de derecho comparado sobre los sistemas normativos que privilegian o no la protección de la información de naturaleza personal sobre el derecho de acceso, destaca que la legislación española sirvió de modelo para países latinoamericanos en cuanto a regular la información personal, pero lo hizo mucho después, con la publicación de la LTBG[565]. Este autor distingue la transparencia, como recurso que *"*favorece la probidad y potencia la participación ciudadana", de la protección de los datos personales, como una herramienta para alcanzar esa transparencia y que a la vez, *"*ampara la intimidad y la autodeterminación informativa"[566]; garantías reunidas en el fallo de la Corte Interamericana de Derechos Humanos por el caso *Claude Reyes*[567], que supone "uno de los avances más importantes en materia de derecho de acceder a la información en poder del Estado"; en que por primera vez un tribunal internacional reconoce el carácter fundamental del citado derecho en su doble vertiente:

> *"(…) como derecho individual de toda persona descrito en la palabra "buscar" y como obligación positiva del Estado para garantizar el derecho a "recibir" la información solicitada, avance que a su vez identifica a la noción de "buscar" como parte de la ciudadanía interesada en la participación en los asuntos públicos (y que se efectiviza, por ejemplo, a través de las leyes nacionales de transparencia en lo público), y a la noción de "recibir" como elemento integrante de la obligación estatal que forma parte de sus deberes como organización representativa"*[568].

El último pilar de la transparencia pública lo constituye la Administración electrónica. Nos invade actualmente una revolución tecnológica y técnica de nuestra sociedad, la llamada sociedad de la información, derivada de las tecnologías de la información y la

565 Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
566 CEA EGAÑA, J.L., *Revista de Derecho y Ciencias Penales*, Universidad de San Sebastián (Chile), 2009, pp. 31-33.
567 Corte Interamericana de Derechos Humanos, Caso Claude Reyes y otros contra Chile, Sentencia de 19 de septiembre de 2006.
568 SANZ SALGUERO, J., "Relación entre la protección de datos personales y el derecho a la pública en el marco del derecho comparado", *Revista Ius et Praxis*, año 22, nº 1, 2016, pp. 341-343.

comunicación (TICs); la cual va impregnando progresivamente todos los ámbitos, al que no escapa la Administración pública, siendo la Ley de Acceso electrónico de los ciudadanos a los Servicios Públicos[569] la que "consagró" el derecho de los ciudadanos a relacionarse electrónicamente con las AAPP, y la obligación de éstas de dotarse de los medios y sistemas para poder ejercerse este derecho. Y, así, en este avance imparable de lo tecnológico, llegamos a lo que debe constituir la norma habitual de las administraciones públicas, la administración electrónica integral, como mejor forma de prestación de los servicios públicos, a través de una mayor eficacia y eficiencia de los mismos y mayor garantía para los administrados.

Dentro de esta etapa modernizadora de la Administración pública española, asistimos a un nuevo estadio de transformación y avance mucho más decidido y de alcance, sobre todo en el ámbito tecnológico. La publicación de la LPAC vino a constituir, sin duda, un momento decisivo en este "*iter*" modernizador; señalando como *"(...) una Administración sin papel basada en el funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a los ciudadanos y empresas, sino que también refuerza la garantía de los administrados*"[570]. De esta forma, mediante la incorporación de medios electrónicos, informáticos y telemáticos, se trata de simplificar, flexibilizar y agilizar procedimientos y trámites administrativos, haciéndolos más simples y cómodos, acercando la administración al ciudadano.

En la LPAC se regulan, entre otras, las siguientes cuestiones: derechos de las personas en sus relaciones con las AAPP, los registros electrónicos, los sistemas de identificación de los interesados en el procedimiento, notificaciones a través de medios electrónicos, emisión de documentos por las AAPP. Por su parte, la LRJSP contempla aspectos, tales como, la identificación electrónica, la firma electrónica del personal público, la obligación de las AAPP de relacionarse electrónicamente entre sí, etc.

Así, la LRJSP y la LPAC, sustituyen (a partir de 2.10.2016), respectivamente, a la Ley 30/1992[571], y a la Ley 11/2007, y sientan el principio de que el uso del medio electrónico

[569] Ley 11/2007, de 22 de junio, Norma básica en los artículos señalados en su disposición final, en vigor hasta el 2 de octubre de 2016.
[570] Preámbulo de la LPAC.
[571] Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

tiene que constituir el medio habitual en las relaciones de las Administraciones con los ciudadanos y de aquellas entre sí.

1.1.1. NORMATIVA REGULADORA DE LA TRANSPARENCIA PÚBLICA

Resulta propio de un Estado democrático la coexistencia de los distintos derechos constitucionales sin que sean necesarios sacrificios injustificados de unos y otros; como sucede con la libertad de expresión e información y los derechos a la intimidad y al honor; de forma que, de igual manera, debería comportarse la coexistencia de los derechos de acceso a la información pública y el derecho a la protección de datos personales; ya que éstos dos últimos han visto reducidos sus desequilibrios (derivados de la regulación del derecho de acceso a los archivos y registros en la Ley 30/1992) gracias a la publicación de la LTBG[572].

La LTBG se dictó con el objeto de ampliar y reforzar la transparencia de la actividad pública, regular y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos, así como las consecuencias derivadas de su incumplimiento (artículo 1).

Así, se encuadran dos de los elementos de la transparencia de la actividad pública: la publicidad activa (o transparencia activa), configurada como una obligación de las Instituciones y AAPP; y el derecho a la información (o transparencia pasiva), que se configura como un derecho de las personas, en base al art. 105.c) CE. En ambos casos, la finalidad de la transparencia es garantizar que los ciudadanos conozcan la organización y funcionamiento de sus instituciones públicas, de forma que la publicidad activa sería el instrumento facilitador de ese conocimiento[573].

Esta ley, ha venido así a establecer un nuevo régimen general de acceso a los archivos y registros públicos; y, a pesar de que viene a suponer un importante avance respecto de la

[572] FERNÁNDEZ RAMOS, S., "Acceso a la información pública versus protección de datos personales", *Revista Española de Derecho Administrativo* nº 184/2017, Editorial Civitas, 2017, pp. 1-29.
En este sentido, entre otros, GUICHOT, E., "Acceso a la información en poder de la Administración y protección de datos personales", *Revista de Administración Pública* nº 173, 2007, pp. 407 y ss.
[573] AEPD. CI/009/2015, de 12 de noviembre de 2015.

legislación anterior, "conserva la tendencia a considerar la transparencia como un mero principio de actuación de las Administraciones públicas, y no tanto como un verdadero derecho de los ciudadanos[574]".

Las distintas CCAA han dictado leyes ampliando e interpretando el contenido básico de la LTBG[575]. De esta forma, junto a las resoluciones, informes y criterios del CTBG[576], nos serán de mucha utilidad las resoluciones y criterios dictados por los respectivos Consejos de transparencia, en especial el de Andalucía.

1.2. TRANSPARENCIA DE LA ACTIVIDAD PÚBLICA SANITARIA

En el ámbito sanitario, la transparencia existe desde que existen datos de contenido sanitario o de salud disponibles sobre la acción pública y sus resultados, para los ciudadanos, investigadores y demás interesados. Así, resulta necesario que las políticas públicas de salud incluyan información sistemática y estructurada, orientada a permitir: de una parte la evaluación de la acción global del sistema sanitario, en cuanto al estudio de variables conjuntas que pueden incidir en el sistema (demografía, nuevas tecnologías, cronicidad, etc.), además de la planificación sanitaria y los elementos de efectividad,

[574] MORETÓN TOQUERO, A., "Transparencia, acceso a la información pública y buen gobierno. Análisis de la cuestión tras la Ley 19/2013", *Revista Jurídica de Castilla y León*, nº 33, 2014.

[575] Leyes autonómicas sobre transparencia:
-Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía. Las reclamaciones se presentan ante el Consejo de Transparencia y Protección de Datos de Andalucía.
-Ley 3/2015, de 4 de marzo, de transparencia y participación ciudadana de Castilla y León. Se reclama ante la Comisión de Transparencia. Estas funciones se han atribuido al Procurador del Común.
- Ley 4/2016, de 15 de diciembre, de Transparencia y Buen Gobierno de Castilla-La Mancha. Firmado convenio con el Consejo de Transparencia y Buen Gobierno (CTBG) para la resolución de las reclamaciones.
- Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana. Se reclama ante el Consejo de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 1/2016, de 18 de enero, de transparencia y buen gobierno de Galicia. Se reclama Ante el Comisión de la Transparencia como órgano independiente adscrito al Valedor do Pobo**.** Esta Comisión de Transparencia será la competente para la resolución de las reclamaciones.
- Proyecto de Ley de Transparencia, Participación Ciudadana y Buen Gobierno del Sector Público Vasco. Se reclama ante la Comisión Vasca de Acceso a la Información Pública
- Cataluña, Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Se reclama ante la Comissió de Garantia del Dret d'Accés a la Informació Pública.
-Ley 4/2016, de 15 de diciembre, de transparencia y buen gobierno de Castilla-La Mancha.
Navarra. Ley Foral 5/2018, de 17 de mayo, de transparencia, acceso a la información pública y buen gobierno. Convenio con el CTBG.

[576] Consejo de Transparencia y Buen Gobierno.

eficiencia, y calidad asistencias; y, de otra, la rendición de cuentas (*accountability*), que implica dar a conocer cómo se produce el proceso de toma de decisiones, además del método utilizado y de los resultados producidos. Como sería el caso, en política sanitaria, de la publicación sobre la utilización de los recursos asistenciales y el catálogo de prestaciones y cartera de servicios incluido en cada centro sanitario del Servicio Regional de Salud correspondiente.

Así, esta rendición de cuentas por los organismos sanitarios tendría influencias en distintos niveles: en el nivel macro (gobierno, parlamento y otras instituciones); meso (centros sanitarios y sus estructuras y aseguradoras); y micro (pacientes y profesionales sanitarios), que sería el nivel estructural quizás más difícil de determinar.

El acceso a los datos públicos de salud garantiza: la transparencia, mediante la consulta de datos que provienen de la fuente; la eficiencia, en cuanto puede influir en el coste de los servicios; y la igualdad de oportunidades, al permitir un acceso global y homogéneo para todos a través de un portal de salud. Por todo ello, la transparencia supone un elemento fundamental en la mejora del sistema sanitario y, por tanto, de los resultados de los centros sanitarios.

Situándonos en el ámbito de la sanidad pública, es preciso hacer referencia a la normativa que regula la transparencia del organismo público sanitario de la Comunidad de Madrid, la cual reconduce las obligaciones de transparencia sobre el núcleo constituido por el buen gobierno y la buena gestión pública de las organizaciones sanitarias. Estas obligaciones, parten de tenerse presente al paciente de forma permanente como centro del sistema, y se desarrollarán a través de los siguientes instrumentos de buen gobierno: profesionalización de la función directiva; fortalecimiento de los órganos de participación (y de asesoramiento); establecimiento de instrumentos de buen gobierno y autonomía de gestión y capacidad de innovación, persiguiendo en todo momento la mayor calidad y eficiencia, más participación y control y una mayor transparencia y rendición de cuentas de la gestión sanitaria[577].

La ley crea las Juntas de Gobierno, como órganos que estarán presentes en todas las organizaciones sanitarias del Servicio Madrileño de Salud, que permitirán una mayor

[577] Ley 11/2017, de 22 de diciembre, de Buen Gobierno y Profesionalización de la Gestión de los Centros y Organizaciones Sanitarias del Servicio Madrileño de Salud.

transparencia en la rendición de cuentas. Además, crea órganos de participación profesional y de representantes públicos (Junta Técnica Asistencial) y de los ciudadanos (Consejos Territoriales de Salud), como medio de hacer más transparente y participativo y de mejor calidad el proceso de toma de decisiones.

Además, se crea un Código de Transparencia, Ética y Buen Gobierno para la sanidad madrileña, aplicable a las jefaturas médicas, de enfermería y de gestión y servicios generales, que deberá "(…) *establecer normas de transparencia para el acceso de todos a la información sobre la sanidad pública madrileña*", además de crear códigos de buenas prácticas para el personal directivo del Servicio Madrileño de Salud.

El art. 20 de esta ley, se refiere a la transparencia (el personal directivo actuará con transparencia y objetividad en el ejercicio de sus funciones) y acceso a la información pasiva, por cuanto las organizaciones del Servicio Madrileño de Salud deberán ofrecer información fidedigna y completa a los ciudadanos sobre los procedimientos, informes, estudios y las razones de sus decisiones; publicándose en la página web institucional el contenido básico de las actas de los órganos previstos en esta ley, respetando la normativa sobre protección de datos. Tratándose de información activa, esta se realizará en formato reutilizable y comprenderá:

"a) La información institucional de la organización: estructura organizativa, Reglamento de Régimen Interior y otras normas internas que se establezcan reglamentariamente; equipo directivo y responsables de unidades, incluyendo información de nombres y datos de contacto en su condición de empleados públicos;

b) La información relativa a actividad, indicadores de calidad asistencial y listas de espera;

c) Información sobre la cartera de servicios;

d) Información económica, presupuestaria y de recursos humanos;

e) Información sobre la contratación pública;

f) Bases de datos y sistemas de información;

g) Información sobre publicaciones de la organización;

h) Información sobre el derecho de acceso a la información: cómo solicitarla y contacto de la persona responsable en cada organización".

2. PUBLICIDAD ACTIVA DE CONTENIDO SANITARIO

Mediante las obligaciones de publicidad activa pública, se reconoce y garantiza el acceso a la información propia de los ámbitos institucional, organizativo y de planificación, así como la que tiene relevancia jurídica, económica, presupuestaria y estadística. Este acceso a la información pública mediante divulgación de la información puede canalizarse:

a) bien de oficio, mediante el Portal de la Transparencia, en el que confluye y centraliza la publicación de toda la información a disposición de los ciudadanos; debiendo considerarse específicamente aquellos datos especialmente protegidos por la legislación de protección de datos personales (RGPD Y LOPDGDD) a la que habrá que remitirse para abordar las distintas situaciones que se planteen;

b) se trataría de la publicidad pasiva o "derecho de acceso a la información pública", en el que, a diferencia de la anterior, la información a solicitar no está parcelizada o categorizada, sino que su contenido sólo se limita a que la misma esté en poder del órgano administrativo, como hemos señalado en el apartado 1 anterior.

La LTBG se refiere exclusivamente a la publicidad mediante internet, señalando que "(…) *la información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas*[578] *o páginas web (…)*"; lo que no debería ser óbice para poder contemplar la existencia de otros medios distintos que, sin embargo, si se

[578] "Es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias (…). El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma; disponiendo el establecimiento de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias": Art. 38.1 LRJSP.

incluyen en distintas leyes autonómicas[579]. Además, la ley no impone, en modo alguno, un deber genérico de uso de medios electrónicos para los ciudadanos, sino que lo declara de vía de comunicación "preferentemente"[580].

En todo caso, esta obligación de publicidad activa se encuentra limitada por el derecho a la protección de datos personales, que si fueran especialmente protegidos (como los datos de salud) exigiría necesariamente utilizar la disociación (art. 5.3.); lo que implica que para los supuestos de existencia de conflicto por la existencia de datos personales en la información que ha de publicarse, se aplica el mismo régimen de límites (excepciones) previsto para el acceso a la información pública (arts. 14 y 15).

Resulta ilustrativa a efectos de valorar la publicidad activa realizada por un Estado europeo la invocación de la STJUE de 9 de noviembre de 2010[581], en la que unos beneficiarios de ayudas agrícolas cuestionan el hecho de que una autoridad estatal publique en su página web datos relativos a su identidad, cuantía, municipio y código de residencia; estimando el tribunal que se trata de una medida desproporcionada, por cuanto para cumplir la finalidad de la transparencia no era necesaria una publicación tan detallada. Pese a tratarse de una sentencia restrictiva supone de positivo aportar una interpretación ajustada de la publicidad en consideración a la extensión de los datos publicados y el medio utilizado[582].

[579] Es el caso de la Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura, que obliga a la publicidad en las web oficiales y también en las distintas unidades de información (arts. 5.1. y 6.2).

[580] AEPD, CI/009/2015, de 12 de noviembre. Sin embargo, tanto el Consejo como la Comisión han defendido la postura contraria, con el apoyo de Suecia, Países Bajos y Grecia.

[581] STJUE de 9 de noviembre de 2010, asunto *Volker und Markus y Hartmut Eifert.*

[582] GUICHOT REINA, E., "Las relaciones entre transparencia y privacidad en el Derecho comunitario ante la reforma de la normativa sobre acceso a los documentos públicos", *Revista Española de Derecho Europeo* nº 37/2011, Civitas, Pamplona, 2011, pp. 16-17.

2.1. SUJETOS OBLIGADOS Y CARACTERÍSTICAS DE LA INFORMACIÓN

Los preceptos de la LTBG son de aplicación a las Administraciones públicas, entidades, organismos públicos, Instituciones del Estado, sociedades mercantiles, fundaciones y asociaciones de constitución y otros sujetos públicos[583], conforme a lo previsto en el artículo 2 de la LTBG[584].

[583] Así, Por ejemplo, la Ley 10/2019, de 10 de abril, de Transparencia y de Participación de la Comunidad de Madrid incluye a:
"1. Partidos políticos, organizaciones sindicales y empresariales, están obligados en todo caso.
2. Entidades privadas que perciban durante el período de un año ayudas o subvenciones públicas financiadas con cargo a los Presupuestos de la Comunidad de Madrid, cuando las ayudas o subvenciones que perciban superen los 60.000 euros o cuando las mismas representen al menos el 30 % del total de sus ingresos anuales, siempre que alcancen como mínimo la cantidad de 5.000 euros" (art. 3).
3. Las entidades privadas que participen en los sistemas públicos de educación, sanidad y servicios sociales mediante conciertos u otras modalidades deberán publicar información específica sobre importes de la 2.1. concesión, condiciones, entre otras cuestiones.
4. Personas o entidades obligadas a inscribirse en el Registro de Transparencia en los términos del Título IV de la Ley 10/2019 de Transparencia y Participación de la Comunidad de Madrid.

[584] Aplicación de la LTBG:
1. A las siguientes Administraciones Públicas
a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla y las entidades que integran la Administración Local.
b) Las entidades gestoras y los servicios comunes de la Seguridad Social, así como las mutuas de accidentes de trabajo y enfermedades profesionales colaboradoras de la Seguridad Social.
c) Los organismos autónomos, las Agencias Estatales, las entidades públicas empresariales y las entidades de Derecho Público que tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad.
d) Las entidades de Derecho Público con personalidad jurídica propia, vinculadas a cualquiera de las Administraciones Públicas o dependientes de ellas, incluidas las Universidades públicas.
2. Al resto de los siguientes organismos públicos (aplicable sólo el título II)
e) Las corporaciones de Derecho Público, en lo relativo a sus actividades sujetas a Derecho Administrativo.
f) La Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con sus actividades sujetas a Derecho Administrativo.
g) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100.
h) Las fundaciones del sector público previstas en la legislación en materia de fundaciones.
i) Las asociaciones constituidas por las Administraciones, organismos y entidades previstos en este artículo.
3. Otros sujetos públicos.
a) Los partidos políticos, organizaciones sindicales y organizaciones empresariales.
b) Las entidades privadas que perciban durante el período de un año ayudas o subvenciones públicas en una cuantía superior a 100.000 euros o cuando al menos el 40 % del total de sus ingresos anuales tengan carácter de ayuda o subvención pública, siempre que alcancen como mínimo la cantidad de 5.000 euros.

En este apartado se incluyen las entidades sanitarias concertadas, las cuales deberán hacer publicación específica sobre cantidades económicas del concierto, condiciones de prestación del servicio, resultados de atención sanitaria, etc.

2.1.1. CARACTERÍSTICAS DE LA INFORMACIÓN

Parece evidente que la información sujeta a las obligaciones de publicidad activa deberá presentarse de una manera clara, estructurada y entendible para los ciudadanos por medios electrónicos. Además, toda la información deberá estar actualizada.

Así, en relación con las condiciones que debe tener la información, el art. 38 LRJSP, al tratar la sede electrónica establece: "(…) *toda la información será comprensible y de acceso fácil y gratuito. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad". En todo caso deberá garantizarse la identificación del órgano titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas*".

Igualmente, la LTBG resalta que "*Toda la información será comprensible, de acceso fácil y gratuito y estará a disposición de las personas con discapacidad en una modalidad suministrada por medios o en formatos adecuados de manera que resulten accesibles y comprensibles, conforme al principio de accesibilidad universal y diseño para todos*" (art. 5.5).

2.2. TIPOLOGÍA Y LÍMITES DE LA INFORMACIÓN

2.2.1. TIPOS DE INFORMACIÓN

En cuanto al tipo de información a publicar, la propia LTBG establece el deber de la Administración de publicar la siguiente información:

a) Información institucional, organizativa y de planificación (art. 8)[585], en la que se incluye las funciones que desarrolla, la normativa aplicable y su estructura organizativa, que comprenderá un organigrama actualizado de los titulares de sus órganos con su perfil y trayectoria profesional.

b) Planes y programas de actuación anuales y plurianuales, en los que se fijen objetivos concretos, así como las actividades, medios y tiempo previsto para su conclusión. Aquí, tanto en el ámbito de la Administración General del Estado como de las CCAA habría que distinguir: entre los Planes de la llamada Administración central de los propios de los organismos autónomos y empresas públicas estatales.

c) Información de relevancia jurídica, en la que se incluyen:

- Las directrices, instrucciones, acuerdos, circulares o respuestas que supongan una interpretación del Derecho o tengan efectos jurídicos.
- Los Anteproyectos de Ley y los proyectos de Decretos Legislativos, cuando se soliciten los dictámenes a los órganos consultivos correspondientes.
- Los proyectos de Reglamentos cuya iniciativa les corresponda. Los dictámenes serán publicados después de emitidos.
- Las memorias e informes que conformen los expedientes de elaboración de los textos normativos, en particular, la memoria del análisis de impacto normativo regulada por el Real Decreto 1083/2009, de 3 de julio.
- Los documentos que, conforme a la legislación sectorial vigente, deban ser sometidos a un período de información pública durante su tramitación (art. 7).

d) Información económica-presupuestaria y estadística, aplicable exclusivamente a las AAPP, a diferencia, de los apartados anteriores, que se aplica a los sujetos incluidos en el ámbito de aplicación del Título I, que deberán publicar, como mínimo los elementos principales del contenido de la siguiente información relativa a los actos de gestión administrativa con repercusión económica o presupuestaria: todos los contratos, convenios suscritos, subvenciones y ayudas concedidas, presupuestos, cuentas anuales, retribuciones de altos cargos y dirigentes de entidades públicas, resoluciones de

[585] Esta información coincidiría con la que con carácter general se suministra a los ciudadanos por las Oficinas de Atención al ciudadano de las distintas Administraciones, y prevista en el Real Decreto 208/1996, de 9 de febrero, por el que se regulan los Servicios de Información Administrativa y Atención al Ciudadano.

autorizaciones de compatibilidad de funcionarios públicos, declaraciones de bienes y actividades de los representantes de entidades locales, estadística para valorar el grado de cumplimiento de funcionamiento de los servicios públicos, relaciones de inmuebles de su propiedad o sobre los que ostenten un derecho real (art. 8).

Los organismos y entidades del sector público deben publicar la identidad de los adjudicatarios de los contratos y convenios que suscriban mencionando a las partes firmantes, en la medida en que se trata de representantes de organismos públicos, es decir, cargos públicos. De forma que, el DNI de los firmantes se considera dato de carácter personal (no especialmente protegido, ni meramente identificativo), estando su publicidad sujeta a las reglas de la ponderación del art. 15 LTBG, en atención al interés público existente en su divulgación y a los derechos de los titulares de los datos[586].

En los llamados regímenes específicos, al aplicarse el criterio previsto por la propia LTBG en materia de publicidad activa y extendido por algunas leyes autonómicas al derecho de acceso, se debería condicionar la aplicación de la LTBG a que se considere este régimen específico de acceso más favorable que el régimen general, sin que ello deba hacerse al margen de la competencia de los órganos de garantía que revisen la actuación de la Administración[587].

La obligación de transparencia también se concreta, a nivel estatal, en distintas normas promulgadas en materia de contratos, subvenciones, presupuestos o actividades de altos cargos[588].

[586] AEPD, CI/004/2015, de 23 de julio de 2015.

[587] FERNÁNDEZ RAMOS, S., "La Transferencia Pública: Pasado, Presente y Futuro". *Revista Aragonesa de Administración Pública*, núm. 51, Zaragoza, 2018, pp. 236-237.

[588] Ley 38/2003, de 17 de noviembre, General de Subvenciones: establece la obligación de los órganos administrativos concedentes de publicar en el diario oficial correspondiente las subvenciones concedidas con expresión de la convocatoria, el programa y crédito presupuestario al que se imputen, beneficiario, cantidad concedida y finalidad o finalidades.
Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa.
Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.
Ley 5/2006, de 10 de abril, de regulación de los conflictos de intereses de los miembros del Gobierno y de los Altos Cargos de la Administración General del Estado que establece que el contenido de las declaraciones de bienes y derechos patrimoniales de los miembros del Gobierno y de los Secretarios de Estado se publicarán en el BOE.

2.2.2. LÍMITES DE LA INFORMACIÓN

Serán de aplicación, en su caso, a la publicidad activa los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15 LTBG. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos (art. 5.3.).

2.3. PORTAL DE TRANSPARENCIA. PORTAL SANITARIO

Con carácter no básico, el art. 10 LTBG contempla la existencia de un Portal único y centralizado, el Portal de Transparencia, en el que se facilitará el acceso a los ciudadanos de toda la información que está obligada a publicar, únicamente exigible para la Administración General del Estado; pudiendo las CCAA crear, o un portal único o bien uno para cada departamento u organismo. La información que se publique en el portal deberá ajustarse a una serie de prescripciones técnicas según se determine reglamentariamente, las cuales deberán adecuarse a los principios de accesibilidad, interoperabilidad y reutilización[589].

Sirva de ejemplo el Portal de transparencia de la Comunidad de Madrid, el cual se encuentra estructurado en torno a los siguientes apartados y subapartados sobre los cuales se va volcando toda la información objeto de publicidad[590]:

1. *Organización y recursos*:

- La institución y su funcionamiento
- Organización
- Altos cargos
- Personal eventual
- Personal al servicio de la Administración

[589] De acuerdo con lo previsto en la Ley 37/2007, de 16 de noviembre, de reutilización de la información del sector público.

[590] https://www.comunidad.madrid/transparencia/

- Relaciones sindicales
- Patrimonio y bienes de la Administración

2. *Servicios y procedimientos*:

- Inventario de Procedimientos y Servicios de la Comunidad
- Listas de espera de servicios públicos
- Quejas y reclamaciones

3. *Presupuestos, contratos y subvenciones:*

- Presupuestos
- Cuentas anuales e informes de fiscalización
- Ayudas, subvenciones
- Contratos
- Convenios
- Datos estadísticos
- Deuda pública

4. *Normativa y planificación*:

- Planes y programas
- Plan anual normativo
- Consulta pública
- Legislación de la Comunidad
- Audiencia e información

- Legislación en tramitación
- Histórico de normas tramitadas

5. *Territorio y transparencia*

- Entidades locales
- Territorio y transparencia

2.3.1. PORTAL SANITARIO

No toda la información de carácter sanitario o de salud que aparece en internet resulta fiable, lo que puede llegar a constituir un problema si no se discriminan adecuadamente las fuentes fiables de información de salud, habida cuenta del carácter tan sensible que tiene este tipo de información. Incluso la información suministrada por proveedores oficiales o autorizados puede llegar a ser comprometida al no poderse garantizar en todos los casos su confidencialidad.

En el portal sanitario o de salud, como fuente de información de este tipo, debe estructurarse la información en función de los sujetos destinatarios de la misma: profesionales sanitarios, pacientes y ciudadanos en general.

Los suministradores o proveedores de la información, como responsables de los contenidos pueden ser tanto, Administraciones y organismos públicos (incluidos centros sanitarios), como sociedades o asociaciones científicas, de pacientes y de profesionales. Todos ellos, deben garantizar que la información volcada en el Portal sea veraz, actualizada y sistematizada para su uso y entendible para los destinatarios de la misma. A la vez que, la seguridad técnica del propio Portal deberá cumplir los estándares técnicos reglamentarios y garantizar la seguridad en las comunicaciones y la confidencialidad en los accesos.

Como ejemplo, se incluye el Portal de Sanidad de la Comunidad de Madrid[591]. El cual se estructura en torno a los siguientes elementos:

1. *Plan anual de contratación 2019 del Servicio Madrileño de Salud (Sermas)*

Esta publicación se refiere a los Contratos Sujetos a Regulación Armonizada (SARA)[592].

2. *Contrato Programa. Centros Sanitarios.*

El contrato programa se constituye como una herramienta que integra los objetivos anuales, enmarcados dentro del planteamiento estratégico a medio plazo del Servicio Madrileño de Salud, definido y singularizado para cada uno de los niveles asistenciales y sus Centros de Gestión, incluido el control y seguimiento de hospitales concesionados.

3. *Observatorio de resultados del Servicio Madrileño de Salud*

En este espacio se pone a disposición de ciudadanos, profesionales y gestores información clave para conocer el estado de salud de los madrileños, así como indicadores de la asistencia sanitaria prestada.

4. *Estado de salud de la población*

En el cual se describe de forma detallada los principales resultados de mortalidad, morbilidad y factores de riesgo, así como los problemas de salud más relevantes de la población madrileña.

5. *Indicadores de Atención primaria y hospitalaria*

Presentan resultados generales de la actividad e indicadores clave de efectividad y seguridad, eficiencia, satisfacción y docencia e investigación; información relevante de la asistencia sanitaria prestada por los centros sanitarios madrileños.

6. *Memorias e informes del Servicio Madrileño de Salud*

[591] Accesible en: https://www.comunidad.madrid/servicios/salud.

[592] Es decir, contratos de suministros y servicios por importe igual o superior a 221.000 € y contratos de obras, de concesión de obras y de concesión de suministros por importe igual o superior a 5.548.000 €.

7. *Plantillas orgánicas de los centros sanitarios del Sermas*. Puestos de trabajo del personal que presta servicios en los centros sanitarios

8. *Listas de espera*

En esta página web se pueden consultar los datos de situación de la lista de espera quirúrgica, de consultas externas y de pruebas diagnósticas/terapéuticas de los hospitales de la red pública de la Comunidad de Madrid, tanto los datos globales, como por hospitales, especialidades y procesos / patologías.

Los pacientes también pueden conocer su situación particular a través de la consulta *on line* personalizada que se ofrece.

9. *Portal estadístico del personal del Servicio Madrileño de Salud*

Proporciona información sobre el total de efectivos de todos los grupos profesionales adscritos a centros sanitarios del Servicio Madrileño de Salud.

10. *Gasto farmacéutico por unidades*. Información sobre los productos de farmacia adquiridos por los hospitales integrados en la red pública del Servicio Madrileño de Salud. Consumo farmacéutico anual de los hospitales públicos de la Comunidad de Madrid.

11. *Encuestas de satisfacción* de los usuarios de los Servicios de Asistencia Sanitaria pública de la comunidad de Madrid.

A través de esta encuesta, se obtiene la información de la percepción y satisfacción de los usuarios sobre la atención recibida.

12. *Pacientes de otras comunidades atendidos en la Comunidad de Madrid.*

13. *Acuerdos del consejo de Administración del SERMAS.*

14. *Reclamaciones, sugerencias y agradecimientos sobre asistencia* sanitaria.

Para el caso de incumplimiento reiterado de las obligaciones de publicidad activa, la LTBG (art. 9), establece que éste se considerará infracción grave, exigiéndose las responsabilidades disciplinarias que resulten de cada normativa reguladora. Antes de esta remisión a una normativa que puede resultar incierta, podría haberse establecido el propio régimen sancionador previsto para el Buen Gobierno. Además, el hecho de que no se fijen

fechas de publicación de la información ni tiempo en el que estará publicada en la página web dificulta enormemente la exigencia de responsabilidades[593].

[593] FERNÁNDEZ RAMOS, S., *Transparencia, Acceso a la Información Pública y Buen Gobierno, Ley 19/2013, de 9 de diciembre*, Thomson Reuters, Pamplona, 2014, p.108.

CAPÍTULO II

DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA DE CARÁCTER SANITARIO Y SU REUTILIZACIÓN, COMO BASES DEL GOBIERNO ABIERTO

1. DERECHO DE ACCESO

"El derecho de acceso a la información pública como garantía de transparencia de la acción de gobierno de los Estados, constituye, en la actualidad, una de las principales herramientas de control público y de lucha contra la corrupción". Al mismo tiempo, asistimos al nacimiento de una nueva forma de gobernar conocida como "*Open Governement*", que, impulsada por el auge de las tecnologías digitales y, tomando como base los principios de transparencia, colaboración y participación, paulatinamente se va implantando en nuestro modelo de sociedad y transformando la actuación de los sistemas democráticos; permitiendo la implantación de nuevas políticas y formas de gestión pública como, por ejemplo, el "*Open Data*" y la implantación de mecanismos de reutilización de los datos públicos"[594]. Así, la publicación de los datos públicos en un portal web en forma estandarizada favorece la transparencia informativa como uno de los objetivos básicos del Open Data.

La constante evolución de las tecnologías, y su cada vez más intensa presencia en casi todos los ámbitos de nuestra vida, indudablemente ha afectado al ámbito de lo público, con nuevos planteamientos sobre el gobierno o administración electrónica, y su evolución a través del *Open Governement*; que traspasa la idea de la transparencia para llegar a la construcción de nuevos espacios de relación entre los poderes públicos y los ciudadanos,

[594] SUBIRANA DE LA CRUZ, S., "Open Governement: transparencia administrativa, derecho de acceso a la información pública, "open data" y reutilización de la información del sector público", *Revista Aranzadi Doctrinal*, nº 2/2016, Editorial Aranzadi, 2016, pp. 1-14.

en los cuales resulta fundamental facilitar, tanto la difusión como el acceso a la información pública, por medios electrónicos.

Por tanto, es objeto de este gobierno abierto no sólo la transparencia sino el fomentar la participación y colaboración de los ciudadanos y empresas; aspecto éste para el cual resulta fundamental que la información pública puede ser reutilizada, para lo que debe proporcionarse en un formato libre.

Así, el Open Data constituye una nueva perspectiva dirigida a poner a disposición de la sociedad los datos públicos a través de formatos de fácil manipulación, para poder ser analizados, reutilizados o distribuidos, con un considerable potencial económico; a través de la generación de nuevos servicios y productos, al mismo tiempo que aumenta la transparencia de la administración (gobierno abierto), la participación y la colaboración ciudadana, generando, además nuevas fuentes de riqueza para ciudadanos y empresas.

Destacar el Portal de Datos Abiertos de Castilla y León, como ejemplo modélico, por su amplitud y sencillez, comprensivo de los Datos sanitarios correspondientes a la información de la epidemia del Covid-19, estructurados en torno a la situación de la epidemia, de los enfermos (por hospitales, por tramos de edad y por zonas) y de los ERTEs por coronavirus[595].

En el ámbito del Derecho de la UE, puede decirse que no existe una norma equivalente al Reglamento 1049/2001[596], aplicable únicamente para las instituciones de la UE, que pueda tener un carácter generalizado de aplicación en los estados miembros en materia de acceso a la información. Por el contrario, existen directivas dictadas para materias concretas

[595] Accesible en: https://datosabiertos.jcyl.es/web/es/datos-abiertos-castilla-leon.html

[596] Reglamento 1049/2001, del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

De ahí, la necesidad de abordar una regulación europea del derecho de acceso a la información, que siguiendo a GUICHOT, debería tomar como premisas las siguientes: así, partiendo del principio general del Derecho comparado de que la normativa sobre acceso constituye ley especial en las demandas de información pública, salvo cuando es el propio interesado el que pide acceso a información que sólo a él le concierne, debería considerarse como una especie de directriz legal, el considerar que los datos más próximos al núcleo duro de la intimidad (básicamente los datos especialmente protegidos) deben ser los más resistentes a la publicidad, a diferencia de los relacionados con la organización y actividad pública que deben someterse a ella[597].

Además, resulta interesante por su influencia en la normativa española la visión del Convenio del Consejo de Europa sobre acceso a los documentos públicos[598], que contiene unos estándares mínimos a cumplir por los estados para el derecho de acceso a la información pública; caracterizándose por un doble enfoque: en el ámbito individual, este derecho es esencial para el desarrollo personal y el ejercicio de los derechos fundamentales de la persona; y en el colectivo, para garantizar la transparencia y el buen gobierno de las AAPP, siendo fundamental fortalecer la confianza de los ciudadanos en las instituciones y favorecer la participación ciudadana.

La legislación española se alineó con otros países europeos en cuanto a la inclusión del derecho de acceso en la Ley 30/1992, aunque, con dos décadas de retraso en relación al tema de la transparencia. El derecho de acceso a los archivos y registros administrativos ordenado en la LPAC resulta plausible como intento, pero carente de fuerza coactiva; haciendo que resulte al poco tiempo mermada su finalidad por el derecho a la protección de datos, consagrado a nivel dogmático como derecho fundamental [599].

[597] GUICHOT REINA, E., "Las relaciones entre transparencia y privacidad en el Derecho comunitario ante la reforma de la normativa sobre acceso a los documentos públicos", *Revista Española de Derecho Europeo* nº 37, enero-marzo 2011.

[598] Aprobado por el Consejo de Ministros del Consejo de Europa el 7 de noviembre de 2008 y abierto a la adhesión de los estados miembros desde el 18 de junio de 2009.

[599] FERNÁNDEZ RAMOS, S., *Acceso a la información pública versus protección de datos personales*, *op.cit*., pp. 4-8.

1.1. NATURALEZA

Sobre la naturaleza del derecho de acceso a la información pública, la CDFUE lo considera como un derecho fundamental de todos los ciudadanos europeos, así como de los residentes o de un estado miembro, y referido al acceso de sus tres instituciones (Parlamento, Consejo y Comisión). Así, en su art. 41, se refiere a este derecho, pero vinculado a una buena administración, el cual incluye entre otros aspectos: "(…) *el derecho de toda persona de acceder al expediente que le afecte, dentro del respeto de los intereses legítimos de la confidencialidad y del secreto profesional y comercial* (…)"; al mismo tiempo que lo reconoce, como derecho ya autónomo e independiente, a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión, para *"(…) todo ciudadano de la UE o toda persona física o jurídica que resida o tenga domicilio social en un estado miembro*".

Para PIÑAR MAÑAS[600], el derecho de acceso a la información pública constituye una de las manifestaciones más importantes de la transparencia (que puede considerarse como un principio de la actuación administrativa), siendo un derecho fundamental relacional o en relación con otros derechos, como el de la libertad de información o la libertad de expresión. Estamos, por tanto, no ante un simple principio de actuación de las Administraciones Públicas, sino que se trata de un derecho relacionado con la necesaria exigencia de rendición de cuentas de los gobernantes, que resulta imprescindible para el libre desarrollo de la personalidad frente a los poderes públicos.

Sigue señalando el profesor PIÑAR MAÑAS, en apoyo de la consideración del derecho de acceso como derecho fundamental, que "no sólo resulta imprescindible para la construcción de una sociedad democrática y participativa (en este sentido son esenciales las sentencias dictadas por el Tribunal de Justicia en el asunto *Access Info Europe*,), sino que es imprescindible para el libre desarrollo de la personalidad frente a los poderes públicos. El ser humano tiene derecho a conocer la actuación de los poderes, incluidas las motivaciones de las decisiones adoptadas, y el uso que se hace de los fondos públicos…"[601].

[600] PIÑAR MAÑAS, J.L., "Transparencia y protección de datos. Una referencia a la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información y buen gobierno", en *Transparencia, acceso a la información y protección de datos*, PIÑAR MAÑAS (Director), Reus Ediciones, Madrid, 2015, pp. 46 y ss.
[601] PIÑAR MAÑAS, J.L., *Revista catalana de derecho público*, nº 49, 2014, pp.7-8.

La naturaleza jurídica del derecho de acceso como derecho fundamental constituyó una gran problemática durante la elaboración de la ley de transparencia; sin embargo, el legislador ha sido totalmente contrario a su reconocimiento, vinculando el derecho de acceso únicamente al art. 105 CE, apartándose de las opiniones doctrinales más cualificadas y de la doctrina jurisprudencial del TEDH.

Para el TEDH el derecho de acceso a la información surge a partir del derecho a la libertad de expresión e información, apoyándose en distintas sentencias[602].

En el ámbito de la jurisprudencia del TJUE[603], todavía no ha dado el paso de considerar el derecho de acceso como un derecho fundamental de carácter autónomo, sin que llegue a pronunciarse sobre su naturaleza, centrándose más en la idea de ser muy importante para la democracia y de que debe garantizarse el acceso más completo posible a los documentos emanados de las instituciones europeas.

No obstante, fuera del ámbito de la UE nos encontramos ante un planteamiento diferente. Así, la doctrina del TEDH ha amparado el acceso a la información pública sobre la base del art. 10 CEDH, que recoge la libertad de expresión en su doble acepción de libertad de opinión y libertad de información, sin incluir, inicialmente, un derecho de acceso a la información pública; aunque posteriormente ha venido concediendo el derecho de acceso a la información pública sobre la base de dicho art. 10 CEDH, a través de la STEDH de 28 de noviembre de 2013.

De esta forma, esta sentencia viene a suponer un avance en la integración del derecho de acceso a la información pública de determinados sujetos, como organizaciones no gubernamentales que persiguen intereses generales, en el derecho a la libertad de información, prevista en el art. 10 CEDH[604].

Por su parte, el TS, sobre la base del art. 105.b) CE, entiende que estamos ante un derecho de configuración legal, un derecho no fundamental, aunque relacionado con el derecho a

602 Sentencia *Társaság a Szabadságjogokért v. Hungary*, de 19 de abril de 2009, y Sentencia *Youth Initiative for Human rights v. Serbia*, de 25 de junio de 2013.

603 STJUE, Sala General, de 22 de marzo de 2011, asunto T-233/, *Access Info Europe contra Consejo*, ratificada por el TJUE de 17 de octubre de 2013, asunto C/280/11 P, *Consejo contra Access Info Europe.*

604 RAZQUIN LIZARRAGA, J.A., "Acerca de la naturaleza del acceso a la información pública (A propósito de la STEDH de 28 de noviembre de 2013)", *Revista Aranzadi Doctrinal*, nº 11/2014, Aranzadi, 2014.

la participación política, con el deber de libertad de información y con el de tutela judicial efectiva[605]. Del mismo modo entiende, que estamos ante una manifestación del principio de transparencia administrativa y otras manifestaciones como el derecho de audiencia o la obligación de motivar las decisiones administrativas; integrando el contenido de uno de los llamados "derechos de última generación": el derecho a una buena administración, contenido en el artículo 41 de la CDFUE de Derechos de la Unión Europea[606].

La posición doctrinal mayoritaria considera que estamos ante un derecho no fundamental, aunque está conectado o tiene relación instrumental respecto de otros derechos fundamentales, en línea con la jurisprudencia[607].

No obstante, hay autores que apoyan su configuración como derecho fundamental[608]. Así, como señala FERNÁNDEZ RAMOS[609], quizás una de las mayores críticas de la ley sea el no calificar el derecho de acceso a la información pública como derecho fundamental incardinado en la libertad de expresión, en un sentido amplio; aunque puede argumentarse su inclusión en la libertad de información del art. 20.1.d) CE. De esta forma, esta configuración de la ley supone situarse en una posición subordinada al derecho a la protección de datos (éste si como derecho fundamental); y que, como veremos, en realidad constituye el principal límite para la efectividad de derecho de acceso. En este caso, estamos ante un derecho de carácter instrumental, por lo que se ejercita no como una finalidad en sí mismo, sino para distintos fines del interesado, sobre los que la Administración no debe entrar a valorar sus finalidades[610].

---

605 STS de 30 de marzo de 1999.

606 STS de 14 de noviembre de 2000.

607 Por todos, POMEZ SÁNCHEZ, L.A., "El acceso de los ciudadanos a los archivos y registros administrativos", INAP, Madrid, 1989, pp.196 y 153; y MESTRE DELGADO, J.F., "El derecho de acceso a archivos y registros administrativos (Análisis del artículo 105.b) de la Constitución)", Civitas, Madrid, 1993, pp. 69 y ss.
Sobre la conexión de este derecho con la jurisprudencia internacional, podemos encontrar un interesante análisis del principio de transparencia en: VALLE ARES GONZÁLEZ, M., "La transparencia en la Unión Europea: una visión comparada. Especial referencia al derecho de acceso a la información pública", Participación educativa, diciembre de 2013, pp. 15-22.

608 Entre ellos, PÉREZ LUÑO, A.E., "Derechos Humanos Estado de Derecho y Constitución", 6ª ed., Tecnos, Madrid, 1999; y SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, M., "Un derecho fundamental a acceder a la información pública", en "El derecho de acceso a la información pública*", Actas del Seminario Internacional Complutense*, Madrid, 2008, pp. 7-41.

609 FERNÁNDEZ RAMOS, S., "Transparencia, Acceso a la Información Pública y Buen Gobierno", *op.cit.*, p. 47.

610 Aquí debe traerse a colación la ejemplar STS de 30 de marzo de 1999, dictada sobre la LRJAP, que señala. "El Abogado del Estado pretende, en síntesis, que condicionemos el reconocimiento del derecho a obtener el acceso al expediente a la real existencia de los presupuestos necesarios para el ejercicio del

En el mismo sentido de apoyo a la consideración como derecho fundamental encontramos autores como GUICHOT REINA[611], que se refiere a la incongruencia que supone el haber considerado como derecho fundamental el derecho a la protección de los datos personales, pese a no estar expresamente reconocido, partiendo del enunciado de un derecho que no parecía pensado para ello (art. 18.4 CE), y, sin embargo, no tratarlo de igual forma para el derecho de acceso a la información pública. Por su parte REY MARTÍNEZ[612], entiende que el derecho de acceso a la información pública es un derecho fundamental "que se halla implícito como nueva manifestación del derecho a recibir información veraz [art. 20.1.d) CE] y que está conectado de modo instrumental con el derecho a participar directamente en los asuntos públicos (art. 23.1 CE)".

La autora RAMS RAMOS[613], sostiene una tesis muy interesante para basar su consideración como derecho fundamental del derecho de acceso a la información pública. Así, partiendo del derecho y de la jurisprudencia internacionales, entiende que el legislador si puede proceder a regular este derecho como fundamental, con el límite de no restringir lo dispuesto en la CE, aunque si puede ampliar su contenido; pero ello, bajo la consideración de que no puede crear derechos fundamentales, ya que esto es patrimonio exclusivo de la Constitución. De esta forma, el legislador sólo puede regular el derecho de acceso a la información pública como derecho fundamental si se encuentra implícito o en conexión con otros derechos fundamentales. De esta forma -sigue sosteniendo RAMS RAMOS con su tesis- considerando que los derechos fundamentales, en nuestro ordenamiento, deben ser interpretados conforme a los tratados y acuerdos internacionales sobre derechos ratificados por España, conforme al art. 10.2 CE; el cual ha permitido a la jurisprudencia del TC adherirse a la propia jurisprudencia del Tribunal Europeo de Derechos Humanos, resulta, por tanto, necesario tener en consideración la jurisprudencia del TEDH. Así, desde 2009, el Tribunal ha dictado tres sentencias que relacionan el

derecho de reversión sobre cuya procedencia el recurrente pretende precisamente informarse. Si accediéramos a esta pretensión estaríamos vinculando, del modo que hemos considerado incompatible con el principio constitucional de acceso a los registros públicos, la posibilidad de obtener información útil al cumplimiento de los requisitos de la reversión (…)"

611 GUICHOT, E., *Transparencia, Acceso a la Información y Buen Gobierno. Estudio de la Ley 19/2013, de 9 de diciembre*, Tecnos, 2014.

612 REY MARTÍNEZ, F., "Quod omnes tangit ab omnibus cognitum esse debet: El derecho de acceso a la información pública como derecho fundamental", *Revista Jurídica de Castilla y León*, nº 33, mayo de 2014, p. 17.

613 RAMS RAMOS, L., "La transformación del derecho de acceso en España: de derecho de configuración legal a derecho fundamental», *Revista Española de Derecho Administrativo*, núm. 160, diciembre de 2013, pp. 155-180.

derecho de acceso a la información pública con el derecho a recibir información del artículo 10 del Convenio de Roma.

Estas sentencias, que sirven de referencia para la defensa de estos postulados, relacionando claramente el derecho de acceso a la información pública con el derecho a recibir información son: La primera Sentencia es *Társaság a Szabadságlogokért* contra Hungría, de 14 de julio de 2007; la segunda es *Kenedi contra Hungría*, de 26 de agosto de 2009; y la tercera sentencia es *Youth Initiative for Human Rights contra Serbia*, de 25 de junio de 2013.

Igualmente, puede establecerse esa conexión entre estos dos derechos por la vía de la normativa internacional, básicamente por el art. 19.2 de la Declaración Universal de Naciones Unidas, el art. 19.2 del Pacto Internacional de Derechos Civiles y Políticos, así como el art. 42 de la CDFUE.

Sin embargo, hay que decir que no estamos ante un derecho fundamental, sino de un derecho constitucional de configuración legal, lo que implica que hay que acudir a las disposiciones que establecen los requisitos para su ejercicio; ya que sólo tendría la condición de derecho fundamental si forma parte del contenido esencial de un derecho fundamental. Tal es el caso[614], entre otros, de los representantes sindicales de los empleados públicos que se integran en la libertad sindical (art. 28 CE). Además, debe contemplarse como "un derecho informativo con sustantividad propia, la libertad de informarse, de acceder a fuentes de información pública, como derecho de libertad (no prestacional o pasivo)"[615].

Resulta preciso señalar que, el hecho de que no se califique como un derecho fundamental, lo que choca, además, con la jurisprudencia del Tribunal Europeo de Derechos Humanos[616], no impide que la realidad de la materialización del derecho de acceso se resienta demasiado, por cuanto en la contienda con el derecho a la protección de datos no importa que tenga éste más preponderancia por el hecho de ser un derecho fundamental, sino que es el juicio ponderativo el que determina cuál de los dos derechos

614 STSJ Cataluña de 5 de octubre de 2010.
615 FERNÁNDEZ RAMOS, S., "Acceso a la información pública versus protección de datos personales", *op. cit.*, pp. 25-27
616 Sentencia de la Gran Sala del TEDH en el caso *Magyar Helsinki Bizottság* c. Hungría, nº 18030/11, de 8 de noviembre de 2016, apartados 149 y ss.

es el aplicable[617]. Además, el que no se considere como derecho fundamental permite poderse desarrollar con más amplitud a través de las leyes autonómicas de transparencia dictadas por las CCAA, dotando, así, al sistema de acceso de una mayor riqueza interpretativa.

La LTBG participa de este enfoque de derecho subjetivo, pero desprovisto de carácter fundamental, siendo una manifestación del principio de transparencia. Así, el art.12 establece que "(…) *todas las personas tienen derecho a acceder a la información pública en los términos previstos en el art. 105.b) CE, desarrollados por esta Ley* (…)".

1.2. LA INFORMACIÓN PÚBLICA COMO CONTENIDO DEL DERECHO DE ACCESO

1.2.1 DERECHO A RECIBIR INFORMACIÓN

Partiendo del ámbito europeo, el derecho de acceso a los documentos y a la información ha tenido una rápida evolución desde su reconocimiento como derecho fundamental en la CDFUE hasta la regulación incluida en el Reglamento 1049/2001, en un camino de difícil recorrido, debido a las propias características del derecho de acceso, así como a la heterogeneidad en las regulaciones nacionales sobre la transparencia pública; que, no obstante, ha ido consolidándose entre las instituciones europeas como instrumento necesario que contrarresta el señalado déficit democrático que padecen las instituciones europeas.

El Reglamento 1049/2001 parte de los principios de transparencia, apertura y proximidad, participación, democracia y respeto a los derechos fundamentales, considerando que deben darse las máximas facilidades para el acceso a la información pública. El objeto del derecho de acceso son los documentos de competencia de la Institución, considerados en un sentido amplio, con independencia del soporte, que incluyen los preparatorios y los de uso interno; y que será tramitado por un procedimiento ágil –a resolver en quince días- pudiéndose recurrir la resolución del mismo. Son titulares de este derecho todos los

[617] MIR PUIGPELAT, O., "El acceso a la información pública en la legislación española de transparencia: crónica de un cambio de paradigma", *Revista Catalana de Derecho Público*, nº 55, diciembre 2017, pp. 48-66.

ciudadanos de la UE, además de todos aquellos que residan o tengan domicilio social en un estado miembro. Las demás personas no tienen este derecho de acceso, pudiendo, no obstante, solicitarlo conforme a las condiciones del art. 4.

En el ámbito sanitario, hay que considerar que la prestación del servicio público aunque fundamentalmente se lleva a cabo por los organismos públicos regionales de salud y empresas y fundaciones de carácter público, sometidos al ámbito de aplicación de la LTBG, existen otros sujetos de carácter privado que en régimen de concertación o de contratación pública se someten a dicha ley; por lo que están obligados a la difusión activa y a conceder la información solicitada de conformidad con sus prescripciones. A este fin, sería conveniente que las Administraciones sanitarias, en los documentos contractuales o de conciertos con las empresas que van a colaborar en la prestación del servicio público sanitario, incluyan previsiones decididas a garantizar la accesibilidad de la información, y que ésta se gestione con criterios propios de los datos abiertos.

El art. 105.b) CE configura a la transparencia como principio de actuación de las AAPP, proyectado especialmente sobre el derecho de acceso a la información en poder de los administrados. Al mismo tiempo, establece una regulación diferida a una futura Ley, aunque la jurisprudencia se ha pronunciado entendiendo que este derecho está dotado por la Constitución de un contenido propio y efectivo, que no puede desconocerse por el legislador y por los llamados a aplicar la norma.

Junto al art. 105.b), la CE, en su artículo 20.1.d), reconoce el derecho a recibir información, como "derecho a informarse" (que supone un planteamiento activo distinto del pasivo del derecho a informar) pudiendo acudir a las fuentes públicas informativas; permitiendo, con ello, que el ciudadano pueda formarse sus propias opiniones y críticas, participando en las discusiones de los asuntos públicos (art. 23 CE)[618], por lo que supone uno de los fundamentos del derecho de acceso. Sin embargo, "(…) *este precepto constitucional es un derecho de libertad que no consiente ser convertido en un derecho*

[618] Estaríamos ante una "participación informada", derivada del principio democrático, al mismo tiempo que supone un contrapeso al ejercicio del poder. MORETÓN TOQUERO, A., "Los límites del derecho de acceso a la información pública", *Revista Jurídica de Castilla y León*, nº 33, mayo 2014, pp.1-24. En relación con la -que parece exagerada- configuración del alcance de la intimidad como absolutamente excluyente del derecho de acceso a los documentos administrativos en nuestro ordenamiento nos remitimos a FERNÁNDEZ SALMERÓN, M., La protección de los datos personales en las Administraciones Públicas, Thomson-Civitas, Madrid, 2003, págs. 177 y ss.

de prestación, como implícitamente pretenden los demandantes (…)"[619]; configurándose este derecho desde la óptica de la comunicación y difusión informativa[620].

Ha sido después de la LTBG, como este derecho se ha visto ampliado a la información pública con la LPAC, a través de su artículo 13, que declara el derecho de todos los ciudadanos de acceder a la información pública, archivos y registros de acuerdo con lo previsto en la LTBG y el resto del Ordenamiento jurídico.

Por tanto, la LPAC diferencia, de una parte el derecho que asiste a toda interesado en un procedimiento a conocer su estado de tramitación, así como distintos elementos del mismo, como el sentido del silencio, el órgano competente para resolver, así como los actos de trámite que hayan sido dictados y a obtener copia de los documentos contenidos en ellos (art. 53); y de otra parte, el derecho de acceso a los archivos y registros administrativos, que se realizará conforme a la LTBG; la cual, pese a que haga coincidir ambos derechos, una cosa es el derecho de los ciudadanos a la información pública y otra distinta el acceso a los ciudadanos a los archivos registros administrativos.

Como recuerda PIÑAR MAÑAS, antes de la aprobación de la LTBG la AEPD emitió el informe de 5 de junio de 2012, en el que "llama la atención a cerca de la necesidad de que la transparencia sea "congruente con los principios que conforman el derecho fundamental a la protección de datos de carácter personal"; de forma que "la divulgación de la información que obre en poder de los sujetos obligados implicará, como punto de partida, la realización de un tratamiento específico sobre los datos de carácter personal que tal información pudiera contener (…); de manera que sólo cabrá conceder el acceso si el mismo es conforme no sólo a la LTBG sino asimismo con la LOPD"[621].

[619] STC 220/1991 de 25 de noviembre, FJ 4.
[620] STC 34/1996, de 11 de marzo, FJ 4.
[621] PIÑAR MAÑAS, J.L., "Transparencia y protección de datos. Una referencia a la Ley 19/2013…", Op.cit., P.58.

1.2.2. ALCANCE DEL TÉRMINO "INFORMACIÓN PÚBLICA"

Respecto de la información pública, el art. 12 de la LTBG, de acuerdo con el principio de accesibilidad máxima, declara la generalidad de los ciudadanos a acceder a toda la información disponible por los poderes públicos (en línea con lo señalado en el Convenio del Consejo de Europa) al señalar en su preámbulo que " (…) *todos los documentos públicos son en principio públicos y solamente pueden ser retenidos para proteger otros derechos e intereses legítimos".* "*Todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105 b) CE, desarrollados por esta Ley*". Es preciso destacar, la ausencia de legitimación para el ejercicio de este derecho.

El propio art. 13 de la Ley define el concepto de información pública, pero no refiriéndose en exclusiva a los documentos, sino a los contenidos o documentos, cualquiera que sea su soporte o formato en poder de los sujetos administrativos incluidos en su ámbito de aplicación[622] (información, entendida no tanto en un sentido material de disposición física como de disposición jurídica, en el sentido de que el administrado, en base a los instrumentos que la ley le proporciona, dispone de las facultades necesarias para su consecución), elaborados o adquiridos en el ejercicio de sus funciones; por lo que incluye aquellos que pueden extraerse por procedimientos o aplicaciones de uso común, y que formen parte de una expediente que esté finalizado a la fecha de la solicitud de la información. De ahí, que, la inadmisión de solicitudes de información, como aquella que "para cuya divulgación sea necesaria una acción previa de reelaboración", deben interpretarse restrictivamente; ya que lo contrario convertiría a la Administración en consultora. Además, el contenido de esta información no queda restringido en modo alguno por estar o no sometida al régimen de publicidad activa"[623].

Dando cumplimiento al deber de información del artículo 13 y 14 de la LTBG, el artículo 11 del LOPDGDD señala que la información básica habrá de ser aportada por el responsable del tratamiento al afectado y debe incluir las fuentes de las que procedieran

[622] Por tanto, el ámbito subjetivo de aplicación de la LTBG se refiere a aquella información pública, archivos y registros en poder de las Administraciones Públicas Territoriales (Administración del Estado, Comunidades Autónomas y Entes Locales) y Entidades de Derecho Público vinculadas o dependientes de las anteriores que ejerzan funciones administrativas.

[623] AEPD. CI/009/2015, de 12 de noviembre de 2015.

los datos; pero no menciona las fuentes accesibles al público, como fueron establecidas en la derogada LOPD:

a) El censo promocional,

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social.

Ante la falta de enumeración de esas fuentes en la LOPDGDD, la AEPD estima aplicables las fuentes de la ley derogada como criterio interpretativo, con la salvedad de que esas fuentes deben provenir de páginas web u otros medios digitales, cuya consulta pueda ser realizada por cualquier persona[624].

Debe señalarse, que, al no estar incluidas en los supuestos previstos en la LOPD, todo lo que se publicaba en internet no tenía la consideración de fuente de acceso público, entendiéndose como una modalidad de comunicación social. En la actualidad, los contenidos de las páginas web, accesibles por cualquier persona, se incluyen como fuente de acceso público, salvo redes específicas de acceso, como redes sociales. Siendo necesario, en todo caso, que los contenidos se adapten al RGPD[625].

[624] Grupo Adaptalia RGPD (2019). Fuentes de Acceso Público en la LOPD y el RGPD. Disponible en: https://www.grupoadaptalia.es/blog/articulos-explicativos-legales/fuentes-de-acceso-publico-en-la-lopd-y-el-rgpd/

[625] AEPD, Informe sobre políticas de privacidad en internet, adaptación al RGPD, septiembre 2018.

1.2.3. APLICACIÓN SUPLETORIA DE LA LEY DE TRANSPARENCIA Y BUEN GOBIERNO (LTBG)

De acuerdo con la Disposición Adicional 1ª LTBG, aquellas materias que disponen de regulación específica de acceso a la información se regirán por su propia normativa, siendo supletoria la LTBG. Esta normativa es la siguiente en función de las materias sobre las que versa:

a) Patrimonio histórico artístico, artículos 57, 58 y 62 de la Ley 16/1985 de 25 de junio, del Patrimonio Histórico español

b) Materias clasificadas y secretos oficiales, la Ley 9/1968 de 5 de abril, de Secretos Oficiales.

c) Datos personales de carácter sanitario. De una parte, los arts. 10 y 23 de la LGS, (modificada por la Ley 26/2011, de 1 de agosto); y, de otra y, con carácter fundamental, la LBAP, en especial el acceso a la Historia Clínica (previsto en el art. 18), que viene a establecer como para proceder a dicho acceso ha de llevarse a cabo una ponderación de los distintos derechos e intereses que intervienen; de forma que se produzca una conciliación de los que son propios del paciente, los que pueden afectar a los profesionales sanitarios intervinientes, así como de terceros y su relación con la normativa sobre protección de datos; ya que tanto el RGPD como la LOGPDD consideran estos datos dentro de una categoría especial, como datos especialmente protegidos, caracterizado por un especial rigor en el tratamiento de los datos de salud, como hemos tenido ocasión de analizar en el título anterior.

En el caso de una solicitud de acceso dirigía al Servicio Andaluz de Salud de que le remitiesen por vía telemática el resultado de unas radiografías realizada, fue denegada con el argumento de que los datos de salud cuentan con un régimen específico de acceso. El CTPD Andalucía[626], señala que, efectivamente " (…) la LBAP contiene un régimen específico de acceso a la información pública en materia de salud –justificado, entre otras motivaciones, en su condición de dato especialmente protegido, que abarca la fijación del contenido del derecho de acceso, la delimitación de los titulares, así como los límites y condicionantes a los que debe sujetarse su ejercicio; criterios que determinan que nos

[626] Consejo de Transparencia y Protección de Datos de Andalucía.

hallemos ante una normativa "específica", aludida por el apartado segundo de la Disp.Adic.4ª LTBG"[627].

d) Archivos de la legislación de Régimen Electoral, artículo 41 de la Ley Orgánica 5/1985, de 19 de junio del Régimen Electoral General.

e) Archivos que sirven a fines exclusivamente estadísticos dentro del ámbito de la función estadística pública, artículos 13 a19 de la Ley 12/1989, de 9 de mayo, de Función Estadística Pública.

f) Acceso a los datos del Registro Civil y del Registro Central de Penados y los registros de carácter público cuyo uso esté regulado por una ley.

g) Derecho de acceso a información medioambiental. Ley 27/2006, de 18 de julio, por la que regula los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente -incorpora las Directivas 2003/4/CE y 2003/35/CE.

En relación con esta Disp.Adic.1ª de la LTBG, señala la AEPD[628] que, dado el carácter de legislación básica que tiene en esta materia, las excepciones a su aplicación en materia de acceso a la información pública deben venir expresamente autorizadas por ella. Así, los apartados 2 y 3 de esta disposición contienen la única excepción prevista en la Ley para la aplicación de sus normas sobre el ejercicio del derecho a la información.

De esta forma, la Disp. Adic.1ª, se refiere a la aplicación supletoria de esta ley en aquellas CCAA que dispongan de legislación específica sobre el derecho de acceso a la información; por lo que, prevalece (aplicación preferente) la legislación autonómica en el ámbito sus competencias sobre la normativa estatal, pero " (…) *sólo cuando la norma autonómica contenga una regulación específica del acceso a la información, por más que regule exhaustivamente otros trámites o aspectos del procedimiento* (…)"[629]. Estos

[627] CTPD Andalucía, RE/132/2016, de 21 de diciembre de 2016.
[628] AEPD, CI/008/2015, de 12 de noviembre de 2015.
[629] *Ibid.*

postulados resultan aplicables igualmente respecto de la legislación ambiental y de la normativa sobre reutilización (apdo.3.).

1.3. INFORMACIÓN PÚBLICA DE CARÁCTER SANITARIO

1.3.1. CARACTERÍSTICAS

En el conjunto del SNS la información constituye un elemento esencial del Sistema que, circunscrita al ámbito asistencial, constituye el presupuesto básico previo a cualquier actuación médica, constituyendo así el consentimiento informado; también puede dirigirse al conjunto de ciudadanos o grupos específicos de ellos. Además, la propia actividad sanitaria, al margen de la información clínica de cada paciente, genera información de todo tipo (estadísticas, estudios, informes, etc.) que son utilizados por el propio Sistema para la planificación, organización y la toma de decisiones.

En un estudio[630] realizado por el Parlamento europeo se destaca las importantes posibilidades que el mercado único digital puede deparar para empresas y ciudadanos reduciendo barreras y costes, de forma que una parte importante de estas posibilidades puede realizarse impulsando la administración y la sanidad electrónicas. Así, los datos de salud estarían implicados en ese proceso de transformación digital, en toda su amplitud.

Hay que señalar como la normativa sanitaria general[631] configura un servicio público de interés general, prestado por organismos incluidos en el sector público, o bien mediante el sector privado, a través de las distintas técnicas de colaboración público-privadas. Este servicio público esencial en el ámbito público se presta en el ámbito del SNS, correspondiendo al Ministerio de Sanidad, básicamente la coordinación del Sistema, a través del Consejo Interterritorial de Salud, y a las CCAA la ejecución de la política sanitaria en su ámbito territorial, correspondiéndoles facilitar el acceso a los datos de salud derivados de la prestación del servicio público sanitario. Son caracteres básicos de

[630] Estudio «Ubiquitous Developments of the Digital Single Market» (Servicios de ubicuidad en el mercado único digital), elaborado por el Departamento Temático A y la agrupación de Wik-Consult, RAND Europe y TNO para la Comisión de Mercado Interior y Protección del Consumidor en 2013 http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/507481/IPOL-IMCO_ET(2013)507481_EN.pdf

[631] Ley General de Sanidad y Ley de Cohesión del Sistema Nacional de Salud.

este sistema; la universalidad, la igualdad, la accesibilidad, la libertad de elección y la financiación pública.

1.3.2. CLASES DE INFORMACIÓN SANITARIA

La información de carácter sanitario o de salud tiene un contenido muy amplio. Así, podemos distinguir: la información asistencial, la información epidemiológica, la información sobre Salud Pública, la información en el Sistema Nacional de Salud, información sobre investigación biomédica, información sobre medicamentos, información para la elección de médico y centro sanitario, y la información sobre listas de espera quirúrgicas.

1) Información de carácter asistencial o clínico. Contenido de la información sanitaria recogida en la LBAP.

La ley contempla entre sus principios básicos la dignidad de la persona y el respeto a su autonomía e intimidad, que orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y documentación clínica (art. 2); reconociendo la confidencialidad de los datos de salud (art. 7), a los que no se podrá acceder salvo autorización legal.

Hay que partir del derecho a la información sanitaria, centrada en el derecho de todo paciente[632] de conocer toda la información disponible sobre su estado de salud física o psíquica o enfermedad, así como todas aquellas circunstancias que pueden afectarle (de modo positivo, actividades de promoción y preventivas, como negativo, situaciones o factores de riesgo) en la toma de decisiones sobre su salud: "*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* (art. 4 LBAP). El paciente podrá determinar que no quiere ser informado, además de que en base a un estado de necesidad terapéutica el médico puede entender que no es apropiado para la salud del paciente informarle.

[632] Paciente: la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de su salud. Art. 3 LBAP.

Este derecho deriva del principio de autodeterminación o de autonomía por el cual es el propio paciente como único responsable de su cuerpo el que decide libremente para adoptar sus propias decisiones relacionadas con la salud, por lo que puede decidir que no quiere ser informado de determinados situaciones o actos médicos.

La emisión de la información podrá ser responsabilidad; bien del médico responsable asignado, o de los que atienden o apliquen una técnica al paciente; o en un ámbito global, los servicios regionales de salud y Ministerio de Sanidad, un servicio sanitario de una especialidad determinada, o bien provenir de una sociedad científica sanitaria.

En cuanto a la información clínica[633] o de salud, sería aquel tipo de información -veraz y suficiente-; bien individualizada, y que, necesariamente, ha de referirse a aspectos concretos relacionados con la asistencia sanitaria o clínica propios de un paciente específico; o colectiva, si se dirige a un grupo social o colectivo concreto, que contiene medidas de ámbito general ante situaciones preventivas o no de una patología determinada (p.ej. información oncológica); en cuyo caso, se encuadra en lo que se denomina "educación para la salud".

Esta información se caracteriza básicamente por tres aspectos: carácter reservado de la información del que deriva el derecho a la confidencialidad de los datos de salud; el consentimiento informado como base jurídica fundamental para el tratamiento de datos de salud, sin perjuicio de las habilitaciones legales y excepciones para situaciones de riesgo; y limitación de usos de la HC a los puramente asistenciales, además de los judiciales, epidemiológicos, de salud pública y de investigación y docencia.

La información clínica formará parte de todas las actuaciones asistenciales. Estará dirigida al paciente como condición previa para la emisión del consentimiento (consentimiento informado), habrá de ser verdadera y comunicarse al paciente de forma comprensible y adaptada a sus necesidades. El titular de la información es el paciente, que la recibirá normalmente de forma verbal, salvo situaciones que entrañen una situación de riesgo para el paciente, en que deberá emitir su consentimiento por escrito; y deberá contener, como mínimo, la finalidad y naturaleza de la intervención, riesgos y

[633] Art. 3 LBAP: "(…) 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".

consecuencias. Podrán también ser informados los familiares y personas vinculadas al paciente, o su representante legal en caso de incapacidad.

El paciente tiene derecho a disponer de una segunda opinión facultativa sobre su proceso clínico, en los términos del art. 28.1 de la Ley de Cohesión. El derecho a la información asistencial se mantiene, aunque el paciente esté hospitalizado.

En el ámbito del Servicio Madrileño de Salud, se ha aprobado un documento sobre el acceso a la documentación clínica, cuyas líneas maestras son las siguientes[634]:

a) Principios aplicables a todos los procedimientos de acceso a información clínica:

- Deber de secreto
- Derecho de acceso personalísimo
- Acceso a los datos por terceros, sólo con el consentimiento del titular
- Contenido mínimo de la solicitud escrita a resolver en un mes.
- El contenido del derecho de acceso incluye el obtener copia de la documentación, en cualquier formato, contenida en la HC, así como información sobre si los datos están siendo tratados, la finalidad del tratamiento, la información disponible sobre el origen de esos datos y las comunicaciones relacionadas con ellos. No comprende la información sobre los profesionales concretos que han accedido a los datos personales.
- Derecho a la tutela de la AEPD.
- Motivos de denegación del acceso a los datos sanitarios: falta de acreditación del interesado o de su representación o autorización; constancia escrita de la negativa del afectado en la propia HC extensiva a familiares del paciente fallecido; solicitud sobre los mismos datos en un período de doce meses sin concurrir interés legítimo; solicitud por tercero, al margen de lo previstos en la ley.

[634] Procedimiento de acceso a la documentación clínica en atención primaria y demás derechos ARCO. Servicio Madrileño de Salud, 4 de febrero de 2015.
Accesible en:
http://www.semg.es/images/stories/recursos/2017/documentos/Derechos_ARCO_AP_v.2.2.pdf

b) Procedimientos de acceso a la documentación clínica (HC):

- Solicitud de copia de documentación clínica, por pacientes, menores e incapaces, y fallecidos.
- Solicitud de acceso, por terceros distintos a los profesionales sanitarios que atienden al paciente, a los datos estrictamente necesarios para el ejercicio de sus funciones; que incluye el acceso por personal no sanitario: de Administración y gestión; que realice funciones de evaluación, acreditación e inspección; acceso por los trabajadores sociales del centro sanitario; por motivos de investigación o docencia (con disociación de los datos clínicos del paciente, separados de los que le identifican); por motivos epidemiológicos y de Salud Pública (conforme a lo dispuesto en la Ley General de Salud Pública).
- Solicitud de acceso por autoridad judicial, Ministerio Fiscal o Fuerzas y Cuerpos de la Seguridad del Estado. Deberá enviarse únicamente la parte de la HC relacionada con el hecho investigado, y en la medida de lo posible disociando los datos identificativos de los clínicos, salvo que expresamente se requiera lo contrario.

2) Información epidemiológica.

El contenido de este tipo de información se recoge en las siguientes leyes:

"*Los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley*" (art. 6 LBAP).

Las AAPP y los Servicios Regionales de Salud llevarán a cabo, entre otras actuaciones: "(…) *La difusión de la información epidemiológica general y específica para fomentar el conocimiento detallado de los problemas de salud*" (art. 18.13 LGS).

Se considera una actividad fundamental del Sistema sanitario la realización de estudios epidemiológicos para orientar con mayor eficacia la prevención de riesgos para la salud (art. 8. 1.LGS).

3) Información sobre Salud pública. Ley General de Salud Pública

Íntimamente ligada a la información epidemiológica se encuentra la información sobre Salud pública, término más amplio en el que queda incluida la información epidemiológica. La prestación de salud pública comprende, entre otras las siguientes actuaciones: "(…) *a) La información y la vigilancia en salud pública y los sistemas de alerta epidemiológica y respuesta rápida ante emergencias en salud pública* (…)" (art. 11.2.2.).

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 (art. 12.1).

Las actuaciones de salud pública deberán ser transparentes. La información sobre las mismas deberá ser clara, sencilla y comprensible para el conjunto de los ciudadanos (art. 3.f). Las informaciones personales que se emplee en las actuaciones de salud pública se adecuarán a lo dispuesto en la normativa sobre protección de datos y en la LBAP (art. 7).

Las Administraciones sanitarias informarán sobre la presencia de riesgos específicos para la salud de la población. Esta información incluirá una valoración de su impacto en la salud, de las medidas que adopten las Administraciones sanitarias al respecto y de las recomendaciones para la población (art. 10).

Se establece que los ciudadanos, con las limitaciones legales establecidas en la ley tendrán el derecho a recibir información:

a) Sobre los derechos que les otorga esta ley, así como sobre las vías para ejercitar tales derechos;

b) Sobre las actuaciones y prestaciones de salud pública, su contenido y la forma de acceder a las mismas;

c) Sobre los riesgos biológicos, químicos, físicos, medioambientales, climáticos o de otro carácter, relevantes para la salud de la población y sobre su impacto. Si el riesgo es inmediato la información se proporcionará con carácter urgente;

d) Toda la información se facilitará desagregada, para su comprensión en función del colectivo afectado, y estará disponible en las condiciones y formato que permita su plena accesibilidad a las personas con discapacidad de cualquier tipo (art. 4).

Bajo el título de "Comunicación en salud pública", el art. 18 de la ley se refiere a que:

"1. Las Administraciones sanitarias velarán por que la información sobre salud dirigida al público sea veraz y cumpla con las previsiones de esta ley, especialmente cuando sea difundida a través de los medios de comunicación social. 2. El Ministerio de Sanidad, Política Social e Igualdad pondrá a disposición de los medios de comunicación y otras organizaciones sociales los criterios de buenas prácticas a que se refiere el artículo 16.3, a fin de que alcancen su máxima difusión. 5. Las Administraciones públicas que desarrollen acciones en materia de comunicación en salud velarán por que la información esté adaptada social, cultural y lingüísticamente a aquellos sectores de la población destinatarios de la misma".

En relación con la información sanitaria en el ámbito laboral, se llevará a cabo conjuntamente con los empresarios y representantes de los trabajadores, con participación de los profesionales sanitarios, de los trabajadores y sus representantes legales y de los empresarios en los planes, programas y actuaciones sanitarias en el campo de la salud laboral. Además, la autoridad sanitaria, de forma coordinada con la autoridad laboral, desarrollara un sistema de información sanitaria en salud laboral que, integrado en el sistema de información de salud pública, dé soporte a la vigilancia de los riesgos sobre la salud relacionados con el trabajo (art. 33).

El Sistema de Información en Salud Pública integrará como mínimo lo siguiente información:

"*a) Las estadísticas, registros y encuestas que midan los condicionantes de la salud: educación, situación social, situación laboral, entorno físico y medioambiental, incluyendo los cambios en el clima, seguridad, demografía, economía, servicios, recursos sanitarios, presencia de contaminantes en las personas y cualquier otra variable que el conocimiento científico y las necesidades de la Administración sanitaria hagan necesaria;*

b) Las estadísticas, registros y encuestas que midan la salud, la calidad de vida y el bienestar de la población;

c) La información sobre políticas y sobre actuaciones de salud pública en todos los ámbitos de acción" (art. 40).

Resulta perfectamente aplicable a la situación actual de epidemia vírica el que: "*Las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población*" (art. 41).

4) Información sobre la cartera de servicios del SNS. Ley de Cohesión del sistema nacional de Salud

La información sanitaria resulta trascendental en el funcionamiento del SNS; tanto en la vertiente de su emisión a pacientes y usuarios del sistema, que "(…) *contendrá información sobre sus derechos y deberes y los riesgos para la salud, facilitará la toma de decisiones sobre su estilo de vida, prácticas de autocuidado y utilización de los servicios sanitarios y ofrecerá la posibilidad de formular sugerencias de los aspectos mencionados* (…)", como de la de servir para la información y la comunicación recíprocas entre la Administración sanitaria del Estado y la de las CCAA; y que "fluirá por todo el sistema sanitario" [635].

El Sistema de información sanitaria, como elemento fundamental del SNS, contendrá, entre otros: datos básicos sobre las prestaciones y la cartera de servicios, población protegida, recursos humanos y financiación, que estará a disposición de los usuarios. El sistema, contendrá, además específicamente la realización de estadísticas para fines estatales en materia sanitaria (art. 53).

Los pacientes y usuarios del SNS tienen derecho a recibir información sobre los servicios y unidades asistenciales disponibles, así como su calidad y los requisitos para su acceso.

Los centros sanitarios deben disponer de una Guía que indique los derechos y obligaciones de los usuarios, las prestaciones disponibles, las características básicas del

[635] Ley de Cohesión y Calidad del Sistema Nacional de Salud, Preámbulo.

centro o servicio, su dotación de personal, instalaciones y medios técnicos. Además, a todos los usuarios se les facilitará información sobre las guías de participación (apenas sin desarrollo efectivo) y sobre sugerencias y reclamaciones.

Será obligación de los servicios de salud informar a los ciudadanos de sus derechos y deberes, de las prestaciones y de la cartera de servicios del Sistema Nacional de Salud, de los requisitos necesarios para el acceso a éstos y de los restantes derechos recogidos en la LGS, la LBAP y en las distintas leyes autonómicas (art. 26).

5) Investigación biomédica. Ley de Investigación Biomédica

En relación con la información a los sujetos participantes en la investigación, el art. 15, señala:

> "1.- Las personas a las que se solicite su participación en un proyecto de investigación recibirán previamente la necesaria información, debidamente documentada y en forma comprensible y cuando se trate de personas con discapacidad de forma adecuada a sus circunstancias.
>
> 2.- La información incluirá el propósito, el plan detallado, las molestias y los posibles riesgos y beneficios de la investigación. Dicha información especificará los siguientes extremos: (…) d) Medidas para asegurar el respeto a la vida privada y a la confidencialidad de los datos personales de acuerdo con las exigencias previstas en la legislación sobre protección de datos de carácter personal; e) Medidas para acceder, en los términos previstos en el artículo 4.5, a la información relevante para el sujeto, que surjan de la investigación o de los resultados totales. En el caso de que no se conozcan estos extremos existirá el compromiso explícito de completar la información cuando los datos estén disponibles.
>
> 3..- Además, las personas a las que se solicite su participación en una investigación serán informadas de los derechos y salvaguardas prescritas en la Ley para su protección y, específicamente, de su derecho a rehusar el consentimiento o a retirarlo en cualquier momento sin que pueda verse afectado por tal motivo su derecho a la asistencia sanitaria".

Existe el deber de informar, poniéndolo a disposición de los participantes si la investigación da lugar a información relevante para la salud de los participantes en el proyecto (art. 26).

En relación con los resultados de la investigación, éstos se comunicarán a los participantes, siempre que lo soliciten. Los investigadores deberán hacer públicos los resultados generales de las investigaciones una vez concluidas, atendiendo a los requisitos relativos a los datos de carácter personal a los que se refiere el artículo 5.5 de esta Ley (art. 27).

6) Información destinada a la elección de centro y profesional sanitario

Los usuarios y pacientes del SNS tienen derecho a la información previa necesaria para la elección de médico y centro sanitario, de acuerdo con lo que se determine por el Servicio Regional de salud correspondiente. Así, la mayoría han establecido normas para la libre elección de médico de primaria, aunque con limitaciones. Para la libre elección de especialista es muy escasa la normativa de autorización.

Destaca la excepción de la Comunidad de Madrid, que ha regulado la libertad total de elección: tanto de profesional sanitario, médico, pediatra y enfermero, como de centro sanitario de atención hospitalaria.

Así, la libertad de elección en el ámbito sanitario sintoniza con una sociedad cada vez más y mejor informada y a la vez más exigente. Es por ello, que la libertad de elección de médico requiere como condición previa una información clara y precisa sobre las prestaciones a las que tiene derecho el paciente dentro de los sistemas de salud[636].

7) Información sobre medicamentos

Comprende básicamente la información dirigida a los pacientes y usuarios principalmente a través de la contenida en el prospecto, ficha técnica y etiquetado de los medicamentos, y que será garantizada por el Ministerio de Sanidad[637] ; de forma que los datos derivados

[636] Ley 6/2009, de 16 de noviembre, de Libertad de Elección en la Sanidad de la Comunidad de Madrid, Preámbulo y Decreto 51/2010, de 29 de julio, del Consejo de Gobierno, por el que se regula el ejercicio de la libertad de elección de médico de familia, pediatra y enfermero en Atención Primaria, y de hospital y médico en Atención Especializada en el Sistema Sanitario Público de la Comunidad de Madrid.

[637] Conforme al art. 15 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.

de las prescripción y dispensación de medicamentos son gestionados por las CCAA; aunque, tratándose de medicamentos que no tienen cobertura pública, la información se queda en las farmacias y laboratorios, que no están sujetos a la LTBG, por lo que el acceso a la información por parte de terceros se ve dificultada.

En cuanto a las garantías y uso racional de los medicamentos y productos sanitarios, existe un sistema de información para apoyo a la prescripción y un sistema que facilita la gestión de las aportaciones de los usuarios que pagan los medicamentos y el control de la prestación farmacéutica de que se trate. Sin duda una utilización avanzada de esta información permitirá, con el respeto a la protección de datos personales, lograr la eficiencia en la prescripción y el consumo de medicamentos, afectando tanto a las administraciones como a los pacientes (adherencias al tratamiento).

1.3.3. INFORMACIÓN SOBRE LISTAS DE ESPERA QUIRÚRGICA

En el ámbito de los servicios públicos de sanidad, la cuestión más problemática sería la de la publicidad de las listas de espera sanitarias. Así, los ciudadanos y pacientes tienen derecho a acceder al contenido de las listas de espera en cuyo contenido esté disociada la información que permita la identificación de su titular. El Real Decreto 605/2003, de 23 de mayo, establece las medidas para el tratamiento homogéneo de la información de las listas de espera en el SNS, refiriéndose al "Portal Estadístico del Sistema Nacional de Salud"; pudiendo los ciudadanos acceder a la información general y a tiempos medios de las listas de espera, que son publicadas en las páginas web de las Consejerías de Sanidad autonómicas.

Tratándose de pacientes, "(…) *tendrán acceso a la información personalizada sobre la espera prevista en relación a su proceso asistencial, que será proporcionada por su servicio de salud (…)*"[638]. Será, por tanto, cada Servicio de salud el encargado de facilitar, de forma específica, la información al paciente sobre la lista de espera en la que se encuentra; sin que se contemple una publicidad generalizada de las listas de espera ante la protección de los datos personales de sus afectados. Así, la Comunidad de Madrid pone a disposición de los pacientes sobre las listas de espera, tanto quirúrgicas, como de

[638] Art. 4.2. del Real Decreto 605/2003.

consultas externas, y de pruebas diagnósticas o terapéuticas, etc., información de interés sanitario y de salud a través de una página web específica de acceso para pacientes [639], en la que, mediante la introducción del DNI y de un código numérico que se facilita al inscribirse, se puede comprobar la situación del paciente en la lista de espera.

Quizás, se echa de menos que estas páginas web específicas no proporcionen más información sobre intervenciones urgentes o trasplantes de órganos, a través de sus respectivas listas de pacientes, lo que redundaría en un menor oscurantismo, posibilitando su no manipulación.

1.4. EJERCICIO DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

El ejercicio del derecho de acceso incluye no sólo acceder a la documentación concreta solicitada, sino también obtener copias y certificados de la misma; aunque la expedición de copias o la transposición de la información a un formato distinto al original podrá dar lugar a exacciones (art. 22.4 LTBG). En consonancia con uno de los objetivos de la LTBG, constituye un ejemplo de buena práctica y de compromiso con la transparencia, el que por el órgano público proporcione la información conforme a los principios de accesibilidad y usabilidad, pudiendo ser valorada y estudiada por quienes tengan interés en ello.

1.4.1. SOLICITUDES DE ACCESO Y PROCEDIMIENTO

El derecho de acceso debe ejercerse mediante petición individualizada de los documentos que se desee consultar sin que quepa formular una solicitud genérica sobre una materia o conjunto de materias. Se pretende de este modo que el ejercicio del derecho no perturbe el regular funcionamiento de los servicios públicos. Así, como advierte el TS:

> "(…) *el derecho de acceso contemplado en el artículo 13 de la Ley 39/2015 no puede ser interpretado de modo absolutamente literal, de forma que cualquier petición en cualquier momento y cualquiera que sea su contenido (se solicitaba la copia de 300 folios) había de ser inmediatamente satisfecha, sino en un contexto sistemático, siendo la propia Ley, en su artículo 37, al regular el*

[639] https://www.sanidadmadrid.org:444/lespera/plogin.jsp

> *derecho de acceso a los archivos y registros, la que establece un límite a las peticiones de los particulares, al señalar que será ejercido de forma que no se vea afectada la eficacia del funcionamiento de los servicios públicos, debiéndose, a tal fin, formular petición individualizada de los documentos que se desee consultar, sin que quepa, salvo para su consideración con carácter potestativo, formular solicitud genérica sobre una materia o conjunto de materias"*[640].

El acceso se realizará preferentemente por vía electrónica, excepto que ello no sea posible o el solicitante haya solicitado otros medios (art. 22). En este sentido, la Ley de Transparencia de Andalucía (LTP de Andalucía) se refiere a que si la información se proporciona en formato electrónico deberá suministrarse en estándar abierto o, en su defecto, deberá ser legible con aplicaciones informáticas que no requieran licencia comercial para esta función[641]. Igualmente, las demás normas autonómicas promueven con carácter general la neutralidad tecnológica y el uso de estándares abiertos sin *copyright*. No obstante, pese a los buenos deseos de la ley, todavía resulta muy incipiente el proceso de implantación de la administración electrónica en nuestro país; lo que, sin duda, dificulta el desarrollo completo de los objetivos de la ley para con los ciudadanos.

Corresponde al solicitante extraer la información y ordenarla como crea conveniente. Si hubiera ya sido publicada en internet, la resolución podrá limitarse a indicar de forma precisa la forma de obtenerla[642]; incluyendo una referencia explícita y determinada al enlace o vínculo para el acceso y, dentro de la página concreta, los epígrafes, capítulos o información relativos a la información solicitada[643], y no una simple indicación genérica[644]. Sin embargo, para la válida utilización de esta vía es preciso que la información en cuestión no esté incluida en ninguna intranet u otro espacio o red de acceso restringido que exija la suscripción del solicitante; por lo que la obtención de una

640 STS de 30 de mayo de 2007.
641 Ley 1/2014, de 24 de junio, de Transparencia pública de Andalucía, Art. 34.1.
642 CTBG, RE/65/2016, de 23 de mayo, nº 151/2016, de 17 de mayo.
643 CTBG, RE/241/2015, de 21 de octubre.
644 CI/009/2015, del CTBG de 12 de noviembre de 2015.

clave de acceso implica un trámite que, además de obstaculizar el acceso a la información, supone unas garantías que ya están previstas en la LTBG[645].

Si la información no pudiera darse en el momento de notificarse la resolución se otorgará en el plazo no superior a diez días. En el caso de oposición de un tercero se produce la suspensión de la ejecución del acceso hasta el transcurso del plazo para interponer el recurso contencioso-administrativo sin que se haya formalizado o se haya resuelto confirmando el derecho a recibir la información.

El procedimiento de inicio de ejercicio de este derecho consistirá en una solicitud nominal dirigida al titular del órgano poseedor de la información o al que se vincule la misma, sin necesidad de motivarla, aunque si se hace podrá considerarse para su resolución[646]. Si el contenido de la solicitud fuera impreciso, se le requerirá al solicitante que, en el plazo de diez, días subsane las deficiencias, con advertencia de que si ello no se realiza se le tendrá por desistido en su petición[647].

Por otra parte, puede señalarse, algún caso en el que se hace muy complicado conseguir el acceso solicitado. Así, por ejemplo, cuando se desea conocer la cantidad de denuncias que se formulan al año por cierto delito, y, de éstas, cuántas dan lugar al inicio de un procedimiento penal, de los procedimientos iniciados, cuántos concluyen en una resolución penal y, de éstas, cuántas se ejecutan. El estudio exhaustivo de los expedientes recientes en poder de la Administración aportaría los datos que, solicitados en su conjunto, supondría un proceso de elaboración, por lo cual la solicitud será inadmitida a trámite en aplicación de la Ley, y si se desea acceder a expedientes en aplicación de la Ley para obtener los datos, se dirá que la información solicitada es excesivamente amplia y afecta a datos personales[648].

En aras de favorecer la comunicación solicitada, las administraciones deberían ser conscientes de que la concesión del acceso solicitado sobre gastos de las mismas, tras una

645 CTBG, RE/393/2016, de 21 de noviembre.
646 Art. 17 LTBG.
647 Art. 39. Ley 10/2019 de Transparencia y de Participación de la Comunidad de Madrid.
648 FERNÁNDEZ RAMOS S., "Transparencia, Acceso a la Información Pública y Buen Gobierno…", *op.cit.*, pp. 25-37.

resolución favorable al solicitante del CTBG, supone ahorrarse la mitad de trabajo que supone el desestimar la solicitud o recurrir en la vía contenciosa.

El CTBG y la AEPD comparten el criterio interpretativo conjunto[649], de que, cuando el acceso a la información favorezca la administración de tareas, conocimiento y recursos de esas instituciones, prevalecerá el interés público sobre los derechos a la protección de datos y a la intimidad, con las excepciones previstas en la LTBG; pero, cuando el acceso no tenga esa finalidad, prevalecerá el respeto al derecho a la protección de datos y a la intimidad: *"*Así, debe recordarse que es la protección del interés general en la transparencia pública, como bien común de nuestra sociedad, la que debe prevalecer frente a solicitudes de información que persiguen otros intereses, de carácter privado o profesional, que no encajan en la finalidad perseguida por la LTBG y, por tanto, no pueden ser considerados superiores*"*[650].

1.4.2. CAUSAS DE INADMISIÓN

Después de presentada la solicitud, debe analizarse por el sujeto público si la documentación presentada cumple o no con las finalidades establecidas en la LTBG; en concreto, mediante la adaptación a los supuestos previstos con carácter general como límites al acceso de la información en el art. 14.1[651], y si fuera de aplicación lo dispuesto en el artículo 18.1, procediendo, en su caso, su inadmisión motivada.

Sobre el carácter restrictivo de la inadmisión de la solicitud de acceso, el TS se ha pronunciado señalando que:

> *"Cualquier pronunciamiento sobre las "causas de inadmisión" que se enumeran en el artículo 18 de la Ley 19/2013, de 9 de diciembre, y, en particular, sobre la prevista en el apartado 1.c) de dicho artículo (que se refiere a solicitudes "relativas a información para cuya divulgación sea necesaria una acción previa*

649 CI/002/2016, del 05 de julio de 2016.

650 Resolución 103/2019 del CTBG de 8 de mayo de 2019. Notificaciones violación de seguridad de datos personales (solicitud desestimada). pp. 14.

651 Resolución de la AEPD 15 de enero de 2019, con cita de la STS de 16 de octubre de 2017, dictada en recurso de casación en el que, entre otras cuestiones, se analizaba el posible perjuicio para los intereses económicos y comerciales de la Corporación RTVE en proporcionar información sobre los gastos derivados de la participación de España en el Festival de Eurovisión.

> *de reelaboración") debe tomar como premisa la formulación amplia y expansiva con la que aparece configurado el derecho de acceso a la información en la Ley 19/2013." (...) "Esa formulación amplia en el reconocimiento y en la regulación legal del derecho de acceso a la información obliga a interpretar de forma estricta, cuando no restrictiva, tanto las limitaciones a ese derecho que se contemplan en el artículo 14.1_de la Ley 19/2013 como las causas de inadmisión de solicitudes de información que aparecen enumeradas en el artículo 18.1".(...) sin que quepa aceptar limitaciones que supongan un menoscabo injustificado y desproporcionado del derecho de acceso a la información*[652].

De acuerdo con el art. 18 LTBG son causas de inadmisión de las solicitudes de acceso las siguientes:

> *a) Que se refieran a información que esté en curso de elaboración o de publicación general*.

El motivo de la inclusión de esta causa radica en la necesidad de que en todo caso se garantice la eficacia de la actuación administrativa, impidiendo el acceso de la documentación que esté en fase: a) de elaboración, por cuanto el contenido inicial puede modificarse posteriormente, por lo que por seguridad jurídica debe impedirse hacerse públicos documentos que no son definitivos; b) de publicación general, o de procedimientos en los que no haya finalizado su tramitación; supuesto en el que es el procedimiento el que no ha finalizado, ya que los documentos integrantes del mismo si tienen carácter final. En este sentido, la doctrina no es unánime en cuanto a la necesidad de que el procedimiento esté o no terminado. Así, un sector entiende que condicionar el derecho de acceso a que el expediente esté terminado es inconstitucional, vaciando de contenido efectivo al derecho de acceso a la información[653].

La Ley de Transparencia de Cataluña limita esta causa de inadmisión "(…) *si la información que se solicita está en fase de elaboración y debe hacerse pública, de*

[652] CTBG, Resolución nº 197/2018, de 29 de junio.
[653] SOTO LOSTAL, S., *El derecho de acceso a la información, el Estado Social y el buen gobierno*, Tirant Lo Blanch, Valencia 2011, pp. 94 y 95.

acuerdo con las obligaciones de transparencia del título II, dentro del plazo de tres meses" (art. 29.1.c).

La mayoría de las leyes autonómicas han completado el contenido del apartado a del artículo 18.1 de la LTBG señalando que "(…) *en las resoluciones de inadmisión porque la información esté en curso de elaboración o publicación general, deberá especificarse el órgano que elabora dicha información y el tiempo previsto para su conclusión*"[654].

> *b) Referidas a información que tenga carácter auxiliar o de apoyo como la contenida en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas*.

Parece lógico que se excluyan documentos que no están terminados, aunque resulta dudoso que lo que son informes y otros documentos de tipo preparatorio, pero terminados, sean excluidos, si se considera su influencia en el conjunto de la decisión final. En este sentido, la Ley madrileña de transparencia excluye considerar como información de carácter auxiliar o de apoyo además de los informes preceptivos a "(…) *aquellos otros documentos que sin serlo hayan servido de forma total o parcial, en su caso, directamente de motivación a resoluciones*" (art. 40.1.b).

Por su parte el CTBG considera que "(…) es el carácter auxiliar o de apoyo de este tipo de información y no el hecho de que se denomine una nota, borrador, resumen o informe interno lo que conlleva la posibilidad de aplicar esta causa de inadmisión". Añadiendo que: "(…) debe tenerse en cuenta que la motivación que exige la Ley 19/2013 para que operen las causas de inadmisión tiene la finalidad de evitar que se deniegue información que tenga relevancia en la tramitación del expediente o en la conformación de la voluntad pública del órgano, es decir, que sea relevante para la rendición de cuentas, el conocimiento de la toma de decisiones públicas y su aplicación. Éstas en ningún caso tendrán la condición de informaciones de carácter auxiliar o de apoyo".

Debemos resaltar como, a la vista del contenido del art. 70.4 de la nueva LPAC, se excluye de formar parte del expediente administrativo la información que tenga carácter auxiliar o de apoyo, como la contenida en *"(…) aplicaciones, ficheros y bases de datos*

[654] Por ejemplo, Ley 10/2019, de 10 de abril, de Transparencia y de Participación de la Comunidad de Madrid, art. 40.2.a)

informáticas, notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas, así como los juicios de valor emitidos por las Administraciones Públicas, salvo que se trate de informes, preceptivos y facultativos, solicitados antes de la resolución administrativa que ponga fin al procedimiento (…)"; lo que puede suponer un entorpecimiento en el normal desarrollo del ejercicio del derecho de acceso a la información pública por los ciudadanos, en la vertiente de acceso al procedimiento administrativo.

Como establece el CTBG[655], es la condición de información auxiliar o de apoyo la que permite, de forma motivada y concreta invocar la aplicación de la causa de exclusión, siendo la enumeración indicada en el apartado b) meramente ejemplarizante, sin que en ningún caso afecte a todos los conceptos enumerados, sino a aquellos que tengan la condición de auxiliar o de apoyo. De forma, que es la finalidad auxiliar o de apoyo y no el hecho de la denominación la que conlleva la posibilidad de aplicar esta causa de inadmisión; por lo que la inadmisión podrá ser declarada cuando concurra alguna de las siguientes circunstancias:

- " Cuando contenga opiniones o valoraciones personales del autor que no manifiesten la posición de un órgano o entidad.
- Cuando lo solicitado sea un texto preliminar o borrador sin la consideración de final.
- Cuando se trate de información preparatoria de la actividad del órgano o entidad que recibe la solicitud.
- Cuando la solicitud se refiera a comunicaciones internas que no constituyan trámites del procedimiento.
- Cuando se trate de informes no preceptivos y que no sean incorporados como motivación de una decisión final".

Respecto del ámbito sanitario, el CTBG señala que una solicitud de estadísticas actualizadas y completas sobre listas de espera en sanidad, supone información disponible

[655] CTBG, CI/006/2015, de 12 de noviembre de 2015.
Este criterio ha sido invocado en la Resolución del CTPD Andalucía nº 241/2018, de 13 de junio de 2018, al entender que se trata de un documento de carácter auxiliar o de apoyo el relativo a un comunicado interno desde el centro educativo de la Delegación de Educación, en el que se informa de unos hechos concretos, sin solicitud de inicio de ninguna actuación administrativa, y sin que, al día de la fecha, haya supuesto el inicio de expediente alguno.

en el Ministerio de Sanidad, sin que se considere como auxiliar o de apoyo, por cuanto es la naturaleza de la información y no su inclusión en alguna de las denominaciones concretas a las que se refiere el art. 18.1.b) LTBG, lo que debe tenerse en cuenta a la hora de la admisión de la solicitud[656].

c) Relativas a información para cuya divulgación sea necesaria una acción previa de reelaboración.

En el ámbito de las instituciones de la UE, éstas no están obligadas a crear documentos para atender una solicitud, de forma que, si la información solicitada implica realizar investigaciones en fuentes distintas, así como elaborar documentos específicos y/o agregación de datos, ello, excede del ámbito del derecho de acceso a la información[657].

Para la Ley catalana de Transparencia, únicamente puede inadmitirse la solicitud "(…) *si para obtener la información solicitada es necesaria una tarea compleja de elaboración o reelaboración.*"[658].

Las distintas leyes autonómicas de transparencia se refieren a la reelaboración, señalando que *"(…) no se estimará como reelaboración que justifique la inadmisión la información que pueda obtenerse mediante un tratamiento informatizado de uso corriente*"[659]. Del mismo modo, para el CTBG[660] el concepto de reelaboración se construye partiendo de la definición de la RAE "volver a hacer algo distinto a lo existente", de forma que puede decidirse la inadmisión de la solicitud por distintos motivos:

1º.- Razones organizativas, funcionales o de coste presupuestario;

656 CTBG, Resolución nº 52-RT/2017 de 9 de mayo.
657 Informe nº 45 de la Comisión de 30 de enero de 2004, sobre la aplicación del Reglamento 1049/2001, de 30 de mayo de 2001, relativo al acceso del público a documentos del Parlamento Europeo, del Consejo y de la Comisión.
658 Art. 29.1.b) LTBG.
659 P.ej. Ley de la Comunidad de Madrid, art. 40.c); Ley andaluza 1/2014, de 24 de junio, art. 30.c); Ley Valenciana 2/2015, de 2 de abril, art. 16.2.b).
660 CTBG, CI nº 7 de 12 de noviembre de 2015. Disponible en la web: file:///C:/Users/blanes_mig/Downloads/Criterio%207_2015_Causas%20inadmisi%C3%B3n%20petici%C3%B3n%20D%C2%BAinformaci%C3%B3n.pdf.

2º.- Información que tenga que elaborarse expresamente haciendo uso de diversas fuentes de información, lo que supone inadmitir solicitudes en las que la información está incluida en fuentes diversas, cuando para acceder a lo solicitado sólo hay que volcar y unir los datos dispersos en un único documento;

3º.- Razones técnicas, o "carencia de medios técnicos necesarios para extraer y explotar la información concreta solicitada, resultando imposible proporcionar la información", ante lo que debe señalarse que no parece justo que la falta de medios tecnológicos de las administraciones afecte a los ciudadanos;

4º.- Formato distinto, si "(…) la petición de un formato concreto distinto al existente podría entenderse como reelaboración, cuando dicho formato no esté en poder de la Administración informante, en todo caso la extracción de la información en formato Excel o Word no entraría en el supuesto de reelaboración".

Ciertamente, una interpretación demasiado amplia del término reelaboración sería un medio muy fácil y socorrido por las Administraciones para inadmitir solicitudes de información, por lo que su recurso debe considerarse de forma restrictiva.

En el ámbito jurisprudencial, señalar como en la resolución del recurso contencioso-administrativo interpuesto por RTVE contra la resolución del CTBG que deniega la solicitud de acceso de información sobre el coste de los canales de RTVE, el Juzgado[661] estima el recurso, anulando la resolución del CTBG en base a los siguientes argumentos:

> *"(…) esta juzgadora comparte la postura de la recurrente pues en efecto, "reelaborar" significa volver a elaborar algo y en el presente caso, para poder suministrar la información solicitada hay que elaborar una "contabilidad" que no existe para cada uno de los canales, porque los costes de los mismos no aparecen desglosados en la contabilidad que presenta la actora y que es pública (…) la información requerida precisaría realizar nuevas operaciones de análisis, agregación e interpretación (…) la ley reconoce el derecho de los ciudadanos al acceso a la información, pero a la información que existe y que está ya disponible, lo que es distinto, de reconocer el derecho a que la Administración produzca, aunque sea con medios propios, información que*

[661] Juzgado Central de lo Contencioso-Administrativo, sentencia de 25 de abril de 2016.

antes no tenía. En el presente caso se está pidiendo una información que a día de hoy no se tiene y cuya obtención no es sencilla pues implica ir desglosando todos y cada uno de los costes de cada canal (…)".

Siguiendo con el alcance del significado de la "reelaboración", el CTPD Andalucía, ha señalado las siguientes directrices aplicativas:

- La reelaboración supone un nuevo tratamiento de la información.
- La reelaboración habrá de basarse en elementos objetivables de carácter organizativo, funcional o presupuestario.
- Existe reelaboración "cuando la información que se solicita, perteneciendo al ámbito funcional del organismo o entidad que recibe la solicitud, deba (…) elaborarse previamente para dar una respuesta, haciendo uso de diversas fuentes de información".
- Así mismo estamos ante una "acción de reelaboración", cuando el organismo o entidad que recibe la solicitud "carezca de los medios técnicos que sean necesarios para extraer y explotar la información concreta que se solicita, resultando imposible proporcionar la información solicitada".
- La noción de reelaboración no supone "la mera agregación o suma de datos, o el mínimo tratamiento de los mismos", ni tampoco equivale a información "cuyo volumen o complejidad hace necesario un proceso específico de trabajo o manipulación para suministrarla a los solicitantes"[662].

Como señala el CTBG, el hecho de tratarse de una información voluminosa, ello no implica que sea precisa una tarea de reelaboración[663].

Por tanto, en el proceso de inadmisión de una solicitud habrá de justificarse concretamente que se está ante un trabajo difícil y complejo de realizar, aun contando con los avanzados medios informáticos de que se dispone.

[662] CTPD Andalucía, RE/64/2016, de 20 de julio.
[663] CTBG, RT/0376/2018, de 4 de febrero de 2018.

d) Dirigidas a un órgano en cuyo poder no obre la información cuando se desconozca el competente.

En relación con este apartado, la regulación de la LTBG resulta un poco confusa e incluso contradictoria. Así, es necesario que la solicitud se dirija al titular del órgano administrativo que tiene en su poder la información (art. 17.1), lo que para el ciudadano normal no es tarea sencilla habida cuenta de la complejidad –frecuente- derivada de los entramados organizativos administrativos públicos. Circunstancia, que puede verse agravada por el hecho de producirse una inadecuada coordinación administrativa y diligencia profesionales, con el resultado final de poder dificultar la agilidad del proceso de resolución de la solicitud; considerando, además, que la resolución se dictará transcurrido un mes desde su recepción en el órgano competente para resolver[664], sin perjuicio de su incremento por otro mes más si se tratara de un volumen o complejidad que así lo requieran (art. 20.1).

Partiendo de que, si el órgano de admisión conoce donde está la información, debe remitírsela, la inadmisión de la solicitud, por tanto, se puede realizar si el órgano que la acuerde entiende que desconoce el competente donde obra la información, pero teniendo que indicar en la resolución el órgano que a su juicio es competente para conocer de la solicitud (art. 18.2); lo que parece incongruente, a no ser que con ello la ley pretenda que se lleven a cabo inadmisiones generalizadas que puedan dejar vacío de contenido el derecho de acceso. Además, la remisión al órgano estimado competente para resolver debería hacerse de oficio y no teniendo que volver a presentarse de nuevo la solicitud por el interesado al habérsela devuelto, lo que a juicio del Tribunal Supremo no es lícito[665].

e) Que sean manifiestamente repetitivas o tengan un carácter abusivo no justificado con la finalidad de transparencia de esta Ley.

[664] Tanto, la ley catalana como la madrileña de transparencia establecen que el plazo de un mes y veinte días, respectivamente, se contará desde la recepción de la solicitud; lo que parece más adecuado, en la medida que, a diferencia de si se computa desde la fecha de recepción del órgano resolutorio, supone un plazo cierto para resolver y, por tanto, mayor agilidad en la respuesta.

[665] STS de 14 de febrero de 2012 "(…) el error cometido por quien presentó el escrito de petición en el departamento llamado "control de reparto" no excusa a la Administración de cumplir con su deber de remitir el escrito de petición que le fue dirigido al órgano competente la Dirección General de Política Universitaria, pues aquella oficina auxiliar de la Sección de Asuntos Generales del Ministerio (control de reparto) debió de encauzar adecuadamente el escrito para que llegase al órgano idóneo para su tramitación y posterior resolución (…)".

Las solicitudes de acceso a la información deben ser razonables en consonancia con el principio general del ejercicio de los derechos conforme a la buena fe. Se plantea la llamada solicitud abusiva cuando se sobrepasa de forma de forma manifiesta el límite normal del ejercicio de un derecho, asociándose el carácter abusivo de la solicitud a la condición de que la petición "no esté justificada con la finalidad de la Ley", que no tiene que relacionarse con el número de solicitudes anteriores (aunque sí si su contenido es reiterativo), pudiendo encuadrarse dentro de alguno de los siguientes supuestos:

- Cuando la solicitud pueda considerarse un abuso de derecho, como lo señala el artículo 7.2 del Código Civil y lo avale la jurisprudencia [666].
- Cuando, de ser atendida, requiriera un tratamiento que obligara a paralizar los servicios administrativos, y así resulte de acuerdo con una ponderación razonada y basada en indicadores objetivos.
- Cuando suponga un riesgo para los derechos de terceros.
- Cuando sea contraria a las normas, las costumbres o la buena fe.

La solicitud estará justificada con la finalidad de la ley, siempre que su interés legítimo esté orientado a: someter a escrutinio la acción de los responsables públicos y a conocer cómo se toman las decisiones públicas, cómo se manejan los fondos públicos y bajo qué criterios actúan las instituciones públicas. Lo que permite concluir (*a sensu contrario*) que no estará justificada esa finalidad: cuando no pueda ser reconducida a ninguna de las finalidades señaladas con anterioridad, previa ponderación razonada y basada en indicadores objetivos; cuando tenga por finalidad patente y manifiesta obtener información que carezca de la consideración de información pública de acuerdo con la definición del artículo 13 de la LTBG; y cuando tenga como objeto o posible consecuencia la comisión de un ilícito civil o penal o una falta administrativa.

Como señala la jurisprudencia comunitaria, el hecho de que una solicitud lleve aparejado un gran volumen de información no exime a las instituciones de realizar un examen concreto de los documentos, de forma que sólo en casos excepcionales en que ello exceda de lo que pueda exigirse razonablemente puede denegarse el acceso. No obstante, deben

[666] STS de 1 de febrero de 2006: "(…) todo acto u omisión que, por la intención de su autor, por su objeto o por las circunstancias en que se realice sobrepase manifiestamente los límites normales del ejercicio de un derecho".

investigarse la posibilidad de otras opciones con el fin de limitar su carga de trabajo y acceder, al menos, en parte a la solicitud[667].

Además, el órgano administrativo siempre dispone de la posibilidad de incrementar el plazo en diez días para poder resolver, conforme al art. 20.1 de la ley[668]; para cuya admisión resulta necesaria la concurrencia de las siguientes circunstancias[669]: a) que el volumen o la complejidad de la información que se solicita lo haga necesario; y b) que la ampliación de plazo, debidamente motivada, sea previamente notificada al interesado (si no lo fuera, el particular podrá entender desestimada su petición).

En relación con esta causa de inadmisión, aplicable a aquellas solicitudes de información cuyo desmesurado volumen o extensión puedan llegar a obstaculizar el normal funcionamiento de la Administración, el CTPD Andalucía, entiende que "esta posibilidad excepcional se sujeta a la observancia de los siguientes requisitos: Así, recae sobre el sujeto al que se dirige la solicitud la tarea de argumentar y acreditar el carácter manifiestamente irrazonable de la carga administrativa que le supone atender a la petición en cuestión, por lo que debe realizarse una motivación explícita de la cantidad desproporcionada de examen e investigación requerida para afrontar la solicitud que, además, debe fundamentarse en datos objetivos.

Por ello, sin ánimo de ser exhaustivos, han de ser tomados en consideración el número y naturaleza de los documentos objeto de la petición, en el bien entendido de que un cuantioso número no predetermina necesariamente una desmesurada carga de trabajo, ya que ésta depende asimismo de la dedicación que precise un adecuado examen de los mismos. Así mismo, cabe ponderar a este respecto, el periodo de tiempo al que se extiende la solicitud, pues la pretensión de abarcar un elevado número de años puede hacer irrazonable una petición que, aisladamente considerada, resultaría plenamente atendible sin mermar el regular funcionamiento de la institución"[670].

[667] STPI, asunto T-2/03, *Verein für Konsumenteninformation* v. Comisión, de 13 de abril de 2005.
[668] RAMS RAMOS, L., *El Derecho de acceso a archivos y registros administrativos*, Reus, Madrid, 2008, p. 473.
[669] CTBG, RT nº 171/2019, de 29 de mayo de 2019.
[670] CTPD Andalucía, Resolución 181/2018, de 23 de mayo de 2018.

En todo caso, la resolución que se dicte debe pronunciarse motivando las razones por las que se considera la solicitud como "manifiestamente repetitiva o abusiva"[671].

1.4.3. EXCEPCIONES AL DERECHO DE ACCESO: LÍMITES ESPECÍFICOS

El propio Reglamento 1049/2001, se refiere, como límite al derecho de acceso a la información, tanto en el Considerando 11[672], como en el art. 4, a lo que constituyen dos tipos de excepciones al derecho de acceso:

a) Absolutas, por las cuales se establece la denegación de acceso cuya divulgación suponga un perjuicio para la protección de: por un lado, el interés público relativo a la seguridad pública, la defensa y los asuntos militares, las relaciones internacionales, o la política financiera, monetaria o económica de la Comunidad o de un estado miembro; y de otro, la intimidad y la integridad de la persona, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales (apartado b); siendo ésta excepción interpretada por el TJUE (caso *Bavarian Lager*)[673], mediante la procedencia de un reenvío a la normativa sobre protección de datos, de forma que tratándose de una solicitud de acceso comprensiva de datos personales resulta de aplicación el Reglamento 45/2001[674], de cuyo Considerando 15 se deriva que el acceso a documentos que contienen datos personales se rigen por las normas de acceso a la información;

b) Relativas, en cuanto están sometidas al examen del interés público en la comunicación de la información, y que, según el apdo.2 del art. 4, las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de: los intereses

---

671 BLANES CLIMENT, M.A., *La transparencia informativa de las Administraciones públicas. El derecho de las personas a saber y la obligación de difundir información pública de forma activa*, Thomson-Reuters Aranzadi, Pamplona, 2014, p. 356.

672 "En principio, todos los documentos de las instituciones deben ser accesibles al público. No obstante, deben ser protegidos determinados intereses públicos y privados a través de excepciones. Conviene que, cuando sea necesario, las instituciones puedan proteger sus consultas y deliberaciones internas con el fin de salvaguardar su capacidad para ejercer sus funciones. Al evaluar las excepciones, las instituciones deben tener en cuenta los principios vigentes en la legislación comunitaria relativos a la protección de los datos personales, en todos los ámbitos de actividad de la Unión".

673 STJUE de 29 de junio de 2010, asunto C-28/08 P, Comisión contra *Bavarian Lager*, por la que se estima el recurso de reposición presentado por la Comisión contra la Sentencia del Tribunal General de 8 de noviembre de 2007, asunto T-194/04, *Bavarian Lager* contra Comisión.

674 Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

comerciales de una persona física o jurídica, incluida la propiedad intelectual; los procedimientos judiciales y el asesoramiento jurídico; el objetivo de las actividades de inspección, investigación y auditoría, salvo que su divulgación revista un interés público superior. Lo que obliga a aplicar los principios de daño efectivo y de interés público preferente en cada caso mediante una ponderación de si se da un interés público superior en la comunicación en relación con la afectación del derecho o el interés protegido con la excepción concreta, y de los perjuicios que pueda suponer la concesión del acceso.

Resulta muy relevante esta sentencia del caso de *Bavarian Lager* en la medida que establece explícitamente una relación entre los dos Reglamentos vistos, al referirse a la aplicación de la normativa sobre protección de datos cuando alude a la excepción del artículo 4.1.b) del Reglamento 1049/2001; de forma que, las solicitudes de acceso a la información deben resolverse conforme a la normativa de acceso a la información y sin que la protección de datos personales pueda considerarse una excepción absoluta al derecho de acceso -a diferencia de cómo lo percibe este Reglamento-, y sin perjuicio de que sean aplicables las normas sobre protección de datos al tratamiento posterior de la información. Por tanto, a falta de un posicionamiento claro sobre los elementos de relación entre ambos derechos en el ámbito comunitario, debe procederse a una aplicación equilibrada de los mismos, sin predominancia de un derecho sobre otro[675].

Sobre esta misma sentencia, y sobre otras relevantes para abordar el conflicto múltiple entre el principio de transparencia y el derecho a la protección de datos de carácter personal y entre este último y el derecho de acceso a los documentos, se pronuncia la profesora NIETO GARRIDO, señalando respecto de la sentencia de *Bavarian Lager* como la que mejor sirve de ejemplo para poner de manifiesto el conflicto entre el derecho de acceso y el de protección de datos y la solución conciliadora propuesta por el TJUE en la sentencia de 29 de junio de 2010, que, previamente, "necesitó de un proceso de ponderación de los bienes jurídicos protegibles por ambos derechos con aplicación del principio de proporcionalidad"[676].

[675] RAMS RAMOS, L.,*Transparencia administrativa y protección de datos personales. V encuentro de Agencias Autonómicas de protección de datos personales*, *op.cit.*, pp. 606-61.

[676] NIETO GARRIDO, Eva, "Transparencia y acceso a los documentos versus derecho a la protección de datos de carácter personal en la reciente jurisprudencia del TJUE", en *Transparencia, acceso a la información y protección de datos*, *op.cit.*, pp. 63-96.

Por tanto, la necesaria ponderación de los intereses legítimos coincidentes en: de una parte, el del solicitante de acceso, que consiste en que se otorgue el acceso solicitado[677]; y de otro, el de los afectados o titulares de datos, interesados en que los mismos sean protegidos, determinará que se considere una comunicación (o tratamiento) lícito, a la vista de lo dispuesto en el art. 6.f) del RGPD[678]. Pudiéndose entender, conforme al art. 6.4. RGPD, que, si en la solicitud no se causan perjuicios en los derechos y libertades de los titulares de datos personales, siempre que no sean especialmente protegidos[679], puede prevalecer el derecho de acceso sobre la protección de datos, incluso si no hubiera consentimiento del titular de los datos.

El RGPD como norma de aplicación directa que, reúne al mismo tiempo, el derecho a la información y a la protección de datos personales -aunque ambos puedan coincidir- no prevé una solución al conflicto aplicativo de ambos derechos, sino que remite al Derecho de la Unión o de los Estados Miembros para su resolución.

Así, el art. 23 del RGPD autoriza a los Estados miembros a establecer medidas legislativas que limiten el alcance de estos derechos mencionados frente al responsable del tratamiento, siempre que tal limitación se articule *" (…) mediante una norma con rango de ley y respete los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática, dictada para salvaguardar la protección de un derecho de otro (el de acceso a la información pública)" (i))*[680].

En ocasiones, parece, que la intimidad y la protección de datos son los límites esenciales y omnipresentes de la transparencia administrativa, cuando en realidad la dimensión de ésta excede del acceso a la información pública, además de que su configuración está

677 RAMS RAMOS, L., "Tratamiento y acceso del público a documentos oficiales", en *Reglamento General de Protección de Datos…*, *op.cit*., pp. 610 y ss.

678 Al que remite la Disp.Adic.10ª de la LOPDGDD, en relación con la comunicación de datos por los sujetos enumerados en el art. 77.1, señalando: "Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679".

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

680 ENÉRIZ OLAECHEA J, "Reglamento General de Datos personales y derecho de acceso a la información pública, o cómo conectar ambos", *Revista Aranzadi Doctrinal*, nº 9/2018, Editorial Aranzadi, 2018, p. 6 y ss.

afectada por diversos límites que no tienen que ser precisamente los derechos fundamentales del art. 18 CE[681].

El hecho de que se establezcan unos límites no deriva de que sea un puro interés de la Administración, sino de la necesidad de protección de la intimidad de las personas; ya que de no establecerse estaríamos ante un acceso indiscriminado a todo tipo de información que dejaría en la absoluta transparencia a la Administración y a los propios ciudadanos; que, de esta forma, quedarían sin protección ante una posible invasión a su intimidad, vulnerando la normativa sobre protección de datos personales. Por ello, resulta necesario, para que la protección de datos surta efecto, la inclusión de límites al acceso a la información pública que contenga datos personales.

Quizás, como señala FERNÁNDEZ RAMOS[682], la LTBG (art. 14), en vez de hablar de límites debería hacerlo como excepciones. Así, la ley no se decanta por un sistema de excepciones absolutas (como en Alemania) sino relativas (como en Gran Bretaña); por cuanto su aplicación no tiene un carácter imperativo, tratándose de un sistema mixto en el que, para cada caso individualizado en el que se plantee una posible excepción al acceso incluye no sólo la prueba del daño (*harm test)*, propia de los sistemas de excepciones absolutas, sino además la técnica de la ponderación de intereses (*balancing of interests*).

El sistema de límites establecidos por la LTBG puede estructurarse de la siguiente forma[683]:

1º.- Se establece un listado único de límites que recoge las materias (art. 14) que pueden entrar en conflicto con el derecho de acceso[684].

2º.- Para resolver el conflicto que pueda justificar la limitación del derecho de acceso, se prevé "un test de daño" (*harm test*), con la finalidad de comprobar el perjuicio que

[681] FERNÁNDEZ SALMERÓN, F., y VALERO TORRES, J., "Transparencia administrativa y protección de datos personales. V encuentro de Agencias Autonómicas de protección de datos personales", *op.cit*., pp. 227 y ss.

[682] FERNÁNDEZ RAMOS, S., *Transparencia, Acceso a la Información Pública y Buen Gobierno, Ley 19/2013, de 9 de diciembre*, *op.cit*., pp. 164-179.

[683] Siguiendo a MORETÓN TOQUERO, *Los límites del derecho de acceso a la información pública*, *op.cit*., pp. 1-24.

[684] En línea con el Criterio del Consejo de Europa en el Convenio sobre Acceso a los Documentos Públicos, que exige que los límites estén contenidos en una ley y sean los necesarios para salvaguardar los intereses relacionados en el art. 3, que tiene una amplia coincidencia con lo que se incluye en el art. 14 LTBG.

el acceso puede producir en el interés a proteger mediante la confidencialidad. Exigiéndose un daño efectivo y no o un mero peligro.

3º.- Una vez advertido el daño potencial a ocasionar con el acceso, se resolverá el conflicto mediante un ejercicio de ponderación (*balancing test*), en el que se considere: de un lado, el interés público en la comunicación de la información; y, por otro, los derechos e intereses incluidos en las materias contenidas en el art. 14; de forma que se decida cual debe prevalecer y ser digno de protección, o en su caso, adoptar un acceso parcial[685], como medida que pueda conciliar los intereses en juego.

Por ello, la formulación de estos límites[686] puede considerarse abstracta, de forma que su aplicación (a los que habrá de añadirse los límites de la protección de datos previstos en el art. 15, como veremos) estará sometida al test de daño y al test ponderación, además de la consideración del principio de maximización del derecho[687], por el que las restricciones deben tener el mínimo alcance necesario, concediéndose en su caso el acceso parcial; por lo que la aplicación de los límites debe estar siempre justificada y motivada, en función de las circunstancias intervinientes en cada caso, y de acuerdo con el principio de proporcionalidad[688].

La propia Constitución exceptúa de la posibilidad de acceso a aquellas materias que afecten a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas. Por ello, la LTBG[689] limita el ejercicio del derecho de acceso a la información cuando ello suponga un perjuicio para las materias que relaciona en el art. 14[690].

---

685 Que a su vez tiene su propio límite en la conservación de la integridad de la información; ya que no procederá si ésta resulta distorsionada o sin sentido.

686 Se trata de límites que van más allá del contenido del art. 105 CE, teniendo conexión con un bien constitucionalmente protegido y viniendo a coincidir prácticamente con los previstos en el Convenio Europeo sobre Acceso a los Documentos Públicos, adoptado por el Consejo de Ministros del Consejo de Europa el 27 de noviembre de 2008

687 GUICHOT REINA, E., *Transparencia y Buen Gobierno, Código Básico Universitario-Codex-Aranzadi*, Edit.Aranzadi, 2014.

688 Vide CI 2/2015 del CTBG, de 24 de junio de 2015, relativo a los límites de aplicación del derecho de acceso.

689 Art. 14 LTBG

690 Art. 14.1 LTBG.

"a) La seguridad nacional.
b) La defensa.
c) Las relaciones exteriores.
d) La seguridad pública.

Además, debe entenderse que el art. 14.1. contempla de forma implícita el acceso parcial a la información solicitada, al señalar que el acceso podrá ser limitado en los casos que determina la Ley; ya que el término "limitado" denota un principio de proporcionalidad, por lo que si se aplica una limitación a una parte del documento debería darse acceso a la parte no limitada[691].

1.4.3.1. **Sentencias sobre la limitación del derecho de acceso**

En el ámbito de la limitación del derecho de acceso en el que nos encontramos, a fin de ilustrarnos sobre ello, resulta interesante invocar los siguientes pronunciamientos judiciales:

ST del Juzgado Central de lo Contencioso nº 98/2017, de 22 de junio de 2017[692]

> *"(...) La ley consagra pues la prevalencia del derecho subjetivo a obtener la información y correlativamente el deber de entregarla, salvo que concurran causas justificadas que limiten tal derecho, a las que se refiere el art. 14, causas que constituyen conceptos jurídicos indeterminados cuya relevancia y trascendencia han de ser concretadas en cada caso, ponderando los intereses en conflicto (...)".*

e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios.
f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva.
g) Las funciones administrativas de vigilancia, inspección y control.
h) Los intereses económicos y comerciales.
i) La política económica y monetaria.
j) El secreto profesional y la propiedad intelectual e industrial.
k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión.
l) La protección del medio ambiente".

691 Refiriéndose al suministro de información parcial en materia medioambiental, la Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente (incorpora las Directivas 2003/4/CE y 2003/35/CE), señala que cuando "La información ambiental solicitada que obre en poder de las autoridades públicas o en el de otro sujeto en su nombre se pondrá parcialmente a disposición del solicitante cuando sea posible separar del texto de la información solicitada la información a que se refiere el artículo 13, apartados 1.d), 1.e) y 2".

692 Sentencia n° 98/2017, de 22 de junio de 2017, del Juzgado Central de lo Contencioso-Administrativo número 11 de Madrid, dictada en el PO 49/2016.

ST igualmente del Juzgado Central de lo Contencioso, de 14 de junio de 2016[693]

> *"(…) Pues bien, a la hora de interpretar tal precepto - 14.1 h-, hemos de tener presente que, la citada Ley, en su Preámbulo, expresamente afirma que la misma configura de forma amplia el derecho de acceso a la información pública y que dicho derecho solamente se verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información o por su entrada en conflicto con otros intereses protegidos".“Así, la finalidad, principio y filosofía que impregna la reseñada Ley, es un acceso amplio a la información pública; y los límites a tal acceso han de motivarse, interpretarse y aplicarse de modo razonado, restrictivo y aquilatado a tenor del llamado, test de daño; a la luz de la determinación del perjuicio que el acceso a determinada información puede producir sobre el interés que se pretende salvaguardar con la limitación".*

1.4.3.2. Examen de las materias relacionadas en el art. 14.1 LTBG

Sobre el criterio de la seguridad pública y la seguridad ciudadana (entendidos como límites similares) en cuanto a actividad dirigida a la protección de personas y bienes y al mantenimiento de la paz ciudadana, se expone el caso de la solicitud de acceso a diferentes datos de actuación del Consejero de la Junta de Andalucía, como lugares de alojamiento, horarios, recorridos y medios usados; lo que supone la posibilidad de aplicación del límite de la seguridad ciudadana, que habrá que evaluar examinando si el daño es concreto, definido y evaluable. Así, en la medida que se aportarían datos de identificación de los lugares de alojamiento del consejero, la comunicación, solamente, de los gastos de alojamiento, supone un riesgo para la integridad personal del titular de la consejería, así como de sus acompañantes y personal de policía que le acompañan; entendiéndose que se trata de un riesgo real. Sin embargo, el resto de datos solicitados no supone riesgo real y efectivo para el desarrollo normal de las actividades de dicho consejero[694].

[693] Sentencia n° 85/2016, de 14 de junio de 2016, del Juzgado Central de lo Contencioso-Administrativo n° 5 de Madrid, dictada en el PO 43/2015.
[694] CTPD Andalucía, RES/34/2019, de 18 de febrero de 2019.

1.4.3.2.1. Intereses económicos y comerciales: Sentencia del Juzgado Central de lo Contencioso de 3 de abril de 2018

La repercusión en los intereses económicos y comerciales (artículo 14.1.h) de los responsables de los tratamientos.

Los "intereses económicos y comerciales" en los que puede basarse la Administración para denegar el acceso, no son sólo intereses propios de la institución pública a la que se le solicita la información, sino que también puede recurrirse a este límite en defensa de los intereses del sector privado, el cual exige que se argumente la existencia de un riesgo real, actual y concreto para estos intereses. Este criterio, se pone de manifiesto en el caso resuelto por el CTPD de Andalucía, relativo a la solicitud de información a una compañía eléctrica "por cambio del término de potencia de forma generalizada a suministros en baja tensión en las ocho provincias de la Comunidad Autónoma de Andalucía"; siendo desestimado el acceso, alegando la necesidad de proteger datos de carácter personal, así como evitar perjuicio a sus intereses económicos y comerciales.

De esta forma, si efectuado el trámite de alegaciones previsto en el art. 19.3 LTBG, la compañía eléctrica no argumenta el por qué puede perjudicar a sus intereses la comunicación del acceso solicitado, debe conducir al acceso a lo solicitado, ya que recae sobre el que se opone a la solicitud "la carga de argumentar la pertinencia de aplicar algún límite que justifique la denegación del acceso a la misma"[695] .

Teniendo en cuenta la ausencia de daño que pudiera provocarse con el acceso y tratándose de información que contribuye a conocer el gasto de una empresa participada en su totalidad con dinero público, la información solicitada debe facilitarse, al entroncar con la razón de ser de la LTBG. La LTBG "ampara el acceso a información de carácter económico de empresas que contraten con organismos públicos y, concretamente, el importe por el que esos servicios son contratados (art. 8) y, ello, sin considerar que el acceso a dicha información pueda considerarse como perjudicial a sus intereses económicos y comerciales"[696].

[695] CTPD Andalucía, RES/042/2016, de 22 de junio de 2016.
[696] CTBG, Resolución nº 197/2018, de 29 de junio.

A nivel jurisprudencial, resulta interesante destacar la resolución del CTBG[697], que acogen en sus fundamentos, entre otras, estas dos sentencias, tanto del Tribunal Supremo, como del Juzgado Central de lo Contencioso de Madrid:

> *(…) Asimismo, la posibilidad de limitar el derecho de acceso a la información no constituye una potestad discrecional de la Administración o entidad a la que se solicita información, pues aquél es un derecho reconocido de forma amplia y que sólo puede ser limitado en los casos y en los términos previstos en la Ley; de manera que la limitación prevista en el artículo 14.1.h/ de la Ley 19/2013 no opera cuando quien la invoca no justifica que facilitar la información solicitada puede suponer perjuicio para los intereses económicos y comerciales"*[698].

Sentencia del Juzgado Central de lo Contencioso de 3 de abril de 2018:

> *"(…) Limitándonos pues al más amplio concepto de "intereses económicos o comerciales", que goza de una protección legal bastante más difusa, resulta que no puede bastar con la invocación genérica de esos perjuicios, sino que debe ser cumplidamente justificada; y dada la interpretación "estricta, cuando no restrictiva" que debe hacerse de estos límites, esta justificación debe referirse a un perjuicio real y efectivo y no a una simple hipótesis o posibilidad de afectación, sin que en este caso pueda considerarse justificada esta afectación"*[699].

[697] *Ibid.*

[698] STS de 16 de octubre de 2017, dictada en recurso de casación en el que, entre otras cuestiones, se analizaba el posible perjuicio para los intereses económicos y comerciales de la Corporación RTVE en proporcionar información sobre los gastos derivados de la participación de España en el Festival de Eurovisión.

[699] Sentencia 42/2018, de 3 de abril de 2018, dictada por el Juzgado Contencioso- Administrativo n° 7 de Madrid.

1.4.3.2.2. Otros límites específicos, sujetos al doble test del daño y ponderación de intereses

- *El secreto profesional y la propiedad intelectual e industrial* (artículo 14.1.j).

En el caso que, por ejemplo, es frecuente que la información contenga códigos fuentes propiedad del responsable.

- *Las funciones administrativas de vigilancia, inspección y control* (artículo 14.1.g).

En aplicación del considerando 87 del RGPD, el cual señala que una notificación de violación de la seguridad de los datos personales "(…) *puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento (…)*".

- *La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva* (artículo 14.f).

Límite que tiene por objeto "(…) garantizar la igualdad de las partes en los procedimientos judiciales tanto ante los tribunales nacionales como internacionales, y puede, por ejemplo, autorizar a una autoridad pública a denegar el acceso a los documentos elaborados o recibidos (por ejemplo, de su abogado) en relación con procedimientos judiciales en los que sea parte. Se deriva del artículo 6 del CEDH, que garantiza el derecho a un juicio justo. Los documentos que no se creen en función de procedimientos judiciales como tales no pueden ser denegados bajo este límite". "Así pues, en línea con este principio, el límite del art. 14.1 f) está llamado a operar esencialmente respecto de los documentos generados específicamente con ocasión del procedimiento judicial de que se trate"[700].

- *La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios* (artículo 14.1.e).

El artículo 32 del RGPD obliga a aplicar medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos, por lo que su falta de implementación podría

[700] CTPD Andalucía, RE/38/2019, de 19 de febrero de 2019.

constituir una infracción tipificada en el artículo 73.g) de la LOPDGDD, que se sancionaría según lo recogido en el artículo 83.4.a) del RGPD.

Tratándose del acceso de documentación judicial, incluidas las sentencias, puede señalarse que según el artículo 235 LOPJ[701] los interesados tendrán acceso a los libros, archivos y registros judiciales que no tengan carácter reservado, mediante las formas de exhibición, testimonio o certificación que establezca la Ley.

Por otra parte, el artículo 266.1 LOPJ determina, en su último inciso, que se permitirá a cualquier interesado el acceso al texto de las sentencias. Ahora bien, el tenor en apariencia concluyente de estos preceptos contrasta con la realidad, que denota no poder afirmar que los libros de registro y archivos judiciales sean una fuente accesible al público. Así, las sentencias judiciales dictadas por los tribunales no son una fuente de acceso público, y es preciso el consentimiento de los afectados para el tratamiento de los datos que en ellas aparecen. Para publicar alguna sentencia, solo podrá hacerse siempre y cuando esté anonimizada, es decir, que no figuren datos personales en la misma[702].

Respecto del ámbito administrativo sancionador, el fundamento de la existencia del propio límite es el mismo que el penal y disciplinario: la protección que debe aplicarse a los expedientes sancionadores, principalmente mientras están siendo tramitados, de forma que la correcta sanción a imponer no sea impedida por la divulgación de la información[703].

Los límites previstos en el art. 14 y 15 (especialmente) de la LTBG son de aplicación igualmente a la publicidad activa, como señala el propio art. 5.3 LTBG.

1.4.4. LIMITACIONES EN EL ÁMBITO SANITARIO

El objetivo de este apartado será delimitar el alcance del derecho de acceso a la información pública sanitaria, regulado básicamente en la LBAP, considerando la

[701] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE núm. 157, del 02/07/1985).
[702] SAN de 31 de marzo de 2015, que desestima el recurso contencioso-administrativo interpuesto contra una Resolución del director de la AEPD de 19-09-2013, sobre derecho de acceso a datos personales.
[703] CTBG, Informe nº 145/2016, de 15 de noviembre.

limitación que establece la normativa sobre protección de datos personales. Por tanto, estamos ante la existencia de dos derechos; uno, un derecho fundamental, el derecho a la protección de datos y, otro, el derecho a la protección de la salud, como derecho básico del que resultan las distintas normativas que regulan la salud y la asistencia sanitaria; que van a verse enfrentados y en conflicto como consecuencia de una solicitud de información sobre datos de contenido sanitario.

Ciertamente, aunque hablemos del derecho a la salud, no existe como tal derecho, pese a su reconocimiento público generalizado. El derecho a la protección de la salud (art. 43.1 y 2 CE), además del art. 41 (Seguridad Social), por su ubicación, supone que estemos no ante un derecho fundamental constitucionalizado, como sería deseable, sino ante un "principio rector" del ordenamiento jurídico; lo que se traduce en que nos situemos ante un derecho de configuración legal (LGS, junto al resto de normas sanitarias), que determina el reparto de las competencias sanitarias entre las distintas administraciones: el Estado, en cuanto a coordinador del sistema sanitario y las CCAA, encargadas de la ejecución de la política sanitaria. Pese a no estar incluido dentro del catálogo de derechos fundamentales, regulado en el Capítulo II del Título Primero, el TC ha interpretado que, en relación con el art. 15 CE, permite considerarlo como un derecho fundamental[704].

Así, el derecho a la protección de la salud, considerado individualmente, en los casos en que resulte necesario, deberá ceder para preservar un interés general o un bien superior constitucionalmente protegido. Así, la salud individual cede ante los casos generales de salud pública que demandan una actuación conjunta para una colectividad (epidemias). De forma que, estas limitaciones se aplican, tanto para el acceso a la información, constituyendo auténticas causas de denegación de la solicitud presentada, como para la difusión de la información, impidiendo su publicación.

Estas limitaciones al acceso a la información se caracterizan por los siguientes elementos:

a) Ausencia de automaticidad. Así, la imposibilidad del acceso a la información debe estar justificada en función de la valoración de los intereses contrapuestos en juego para cada caso, de forma que si la denegación no se lleva a cabo sin un equilibro previo será antijurídica. Por ello, los motivos de denegación deben interpretarse de forma restrictiva.

[704] SSTC 62/07 de 27 de marzo y 160/07, de 2 de junio.

b) Falta de obligatoriedad, ya que tienen un carácter de recomendación o sugerencia, lo que implica que no son necesarias, pudiendo o no incluirse. Sin embargo, se trata de una lista cerrada de casos limitativos del acceso a la información, sin que puedan incorporarse nuevos supuestos por parte de los estados miembros[705].

c) Cabe la posibilidad de que la Administración solicitante conceda el acceso parcial de la información solicitada en los supuestos en los que los límites contenidos en el art. 14 LTBG no afecten al total de la información; en cuyo caso, la parte no afectada podrá ser objeto de acceso, denegando la restante[706].

En el caso de una solicitud de acceso a "todas y cada una de las inspecciones de sanidad hechas en bares, restaurantes, cafeterías, discotecas y pubs de Madrid, entre el 1 de enero de 2016 y el 20 de julio de 2018, con inclusión del nombre y dirección del local, sobre qué era la inspección y su resultado, y si hubiese deficiencias, información sobre ellas", el CTBG, en base al CI/002/2015, de 21 de mayo de 2015, entiende que en principio la información referida al establecimiento puede estimarse que la misma no contiene datos personales; ya que el nombre del establecimiento es una marca comercial y las personas jurídicas se sitúan al margen de la LOPD (norma vigente en el momento de redactarse el informe del CTBG). Además, la dirección, lo es de un establecimiento, no de una persona física, y finalmente los resultados de la inspección consisten en describir los aspectos sobre salud e higiene, pero del local, lo que no es probable que contenga datos personales, por lo que puede accederse a lo solicitado[707].

1.4.5. CONSEJO DE TRANSPARENCIA Y BUEN GOBIERNO

La aportación más destacada de esta ley[708] ha sido la creación de los órganos de garantía del derecho de acceso a la información pública, como el Consejo de Transparencia y Buen Gobierno (CTBG), "un organismo que ejerce de juez cuando el ciudadano y la

[705] STJUE 178, de 9 de septiembre de 1999.

[706] Art. 16: "En los casos en que la aplicación de alguno de los límites previstos en el artículo 14 no afecte a la totalidad de la información, se concederá el acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida".

[707] CTBG, RT/ 0376/2018, de 4 de febrero de 2018.

[708] FERNÁNDEZ RAMOS, S., "Transparencia, Acceso a la Información Pública…" *op.cit*., p. 47.

Administración no se ponen de acuerdo sobre qué datos deben ser públicos y cuáles no"[709]; cumpliendo sus funciones a pesar de limitaciones financieras y organizativas.

Esta importancia se corresponde con la dedicación de todo un título completo (III) de la ley, que le configura con un organismo con personalidad jurídica propia que actúa con autonomía y plena independencia; siendo su misión "(…) *velar por el cumplimiento de las obligaciones de publicidad, salvaguardar el ejercicio del derecho de acceso a la información pública (*…)" (art. 34). Anualmente, elaborará una memoria sobre sus actividades que será presentada ante las Cortes por el Presidente del Consejo (art. 40).

Además de sus funciones de asesoramiento y demás previstas en el art. 38, la más trascendente es la de resolver las solicitudes o reclamaciones ante el propio CTBG, previstas en el art. 24. En este sentido, la competencia de resolver estas reclamaciones se circunscribe al ámbito de resoluciones provenientes de la Administración General de Estado; ya que las que se refieren a reclamaciones propias de los órganos de las CCAA o de las Entidades Locales, el competente para resolverlas será el propio órgano creado al efecto por las CCAA.

Así, pese, a que éstas podrían encomendar mediante convenio esta competencia al CTBG, la mayoría de Comunidades han creado este órgano específico[710]: Andalucía, Aragón, Canarias, Cataluña, Comunidad Foral de Navarra, Comunitat Valenciana, País Vasco y Región de Murcia. Hay Comunidades que han encargado esta competencia a organismos que ya existían: Galicia (Valedor do Pobo), Castilla y León (Procurador del Común) e Illes Balears (Abogacía de la Comunidad Autónoma). Por último, Cantabria, Castilla-La Mancha, Comunidad de Madrid, Extremadura, La Rioja, Principado de Asturias y las ciudades de Ceuta y Melilla no han creado su propio órgano independiente

[709] SEVILLANO, E. "El Consejo de Transparencia sufre para ejercer su función de vigilancia del poder: Con un 22% menos de presupuesto, sin nombrar presidente y sin reglamento, el órgano ha visto duplicada su carga de trabajo", artículo de El País, 1 de julio 2018. Disponible en: https://elpais.com/politica/2018/06/20/actualidad/1529505765_330795.html

[710] P.ej. la Comunidad de Madrid, en su Ley 10/2019, de 10 de abril, de Transparencia y de Participación de la Comunidad de Madrid, creó el Consejo de Transparencia de esa Comunidad, que deberá estar constituido en el plazo de seis meses desde la entrada en vigor de la ley.

de transparencia y han firmado un convenio con el Consejo de Transparencia estatal para que atienda las reclamaciones que afectan a sus territorios[711].

En cuanto a las reclamaciones tramitadas, el Consejo de Transparencia ha recibido 1638 reclamaciones que afectan a las CCAA. De ellas, 1530 sí se han tramitado, porque corresponden a CCAA que han firmado convenio y, por tanto, las atiende y resuelve el Consejo de Transparencia estatal. El reparto es el siguiente: el mayor número corresponde a la Comunidad de Madrid (611), seguido de Castilla-La Mancha (290), Cantabria (198), Extremadura (155) y Principado de Asturias (141). Los ciudadanos del resto de territorios han reclamado menos: La Rioja (35), Ceuta (53) y Melilla (47).[712]

La organización y funcionamiento del Consejo se rige por el Real Decreto 919/2014, de 31 de octubre por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno.

Por su relación con la salud, podemos hacer referencia a la siguiente resolución del CTBG[713]:

1.- Así, por parte de una ciudadana se presentó ante la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) solicitud de información dirigida a conocer "el número de casos notificados y en investigación de los incidentes asociados al producto *Ala Octa*: análisis toxicológicos, ensayos químicos, nombre de los expertos e informes de resultados…"; siendo denegada por la Agencia alegando que la información está en fase de información, a la vez que indica que existe una norma específica (Real Decreto 1591/2009, por el que se regulan los productos sanitarios) para solicitar el acceso que se aplica preferentemente a la ley de transparencia.

2.- Presentada reclamación, el CTBG la estima parcialmente, en base a que la norma citada contiene una previsión específica, que, aunque, no es de acceso a la información,

[711] Encuentro entre el Consejo de Transparencia y Buen Gobierno y los Consejos y Comisionados de Transparencia de ámbito autonómico, 8 de mayo de 2019. Disponible en: https://www.consejodetransparencia.es/ct_Home/comunicacion/actualidadynoticias/hemeroteca/2019/Primersemestre/20190508.html#.XpMAYf0zYnQ.

[712] Datos hechos públicos en el Encuentro entre el Consejo de Transparencia y Buen Gobierno y los Consejos y Comisionados de Transparencia de ámbito autonómico, de 8 de mayo de 2019.

[713] CTBG, Resolución 46/2018, de 30 de abril de 2018.

si es de confidencialidad; lo que implica un límite al derecho de acceso "en relación a la metodología utilizada en los ensayos del laboratorio fabricante que pudiera contener secretos comerciales, así como a los avances en la investigación en curso". Entendiendo que no afecta a la protección de datos personales "el hecho de identificar a los expertos participantes, por haberse creado una situación de alarma social que afecta sustancialmente a la salud pública, lo que presupone la existencia de un interés público superior a tener en cuenta".

3.- Impugnada la resolución del CTBG ante la jurisdicción contencioso-administrativa, por parte del Ministerio de Sanidad, Servicios Sociales e igualdad (al que se adscribe la AEMPS), se dicta sentencia desestimatoria por parte de la Audiencia Nacional[714]; en base a considerar que existe una justificación proporcionada y adecuada para facilitar los datos solicitados, por cuanto "la información solicitada concernía y concierne a aspectos que afectan no solamente a la salud de la solicitante y de otras personas concretadas en esos casos, sino de un indudable interés público puesto que tiene un alcance general en orden a la protección del derecho fundamental a la protección y prevención de la salud humana y a la integridad física de otros posibles afectados por estas incidencias". Además, añade la Sala para su apoyo jurídico, que el TS (sentencia de 16 de octubre de 2017), que esos: "… límites previstos se aplicarán atendiendo a un test de daño (del interés que se salvaguarda con el límite) y de interés público en la divulgación (que en el caso concreto no 11 prevalezca el interés público en la divulgación de la información) y de forma proporcionada y limitada por su objeto y finalidad. Asimismo, dado que el acceso a la información puede afectar de forma directa a la protección de los datos personales, la Ley aclara la relación entre ambos derechos estableciendo los mecanismos de equilibrio necesarios"

Por último, en relación con la cuestión de si la información parcial facilitada puede vulnerar la LOPDGDD, por propiciar el nombre o identificación de aquellas personas que, en este caso concreto, participaron como expertos en el panel para la evaluación clínica individualizada de los casos; señala sentencia no compartir la tesis de la Administración demandante "*de que el deber de identificación se refiere tan sólo al órgano en sí 12 mismo considerado y no a la identidad de los miembros del mismo, es*

[714] SAN nº 77/2019, del Juzgado Central de lo Contencioso-Administrativo, de fecha 19 de junio de 2019.

decir, de las personas, puesto que una vez conocido el órgano competente sobre la actividad subsiste el mismo problema de saber quién y con qué condiciones personales han sido ponderadas técnica o médicamente las incidencias que tienen relación con la salud, la prevención, o la integridad física de los ciudadanos".

4.- Apelada la sentencia por el Ministerio de Sanidad, Servicios Sociales e Igualdad, la Audiencia Nacional, desestima la apelación[715], en base a, entre otras las siguientes consideraciones:

> "*El régimen contenido en el Real Decreto 1591/2009 no excluye la aplicación de la Ley 19/2013, pues si bien contempla un criterio de confidencialidad, lo hace con carácter de previsión general en relación con los productos sanitarios y sus accesorios de conformidad con las previsiones establecidas en su artículo 1, estableciendo, como señala la exposición de motivos, un sistema de vigilancia sobre los mismos con objeto de evaluar los incidentes adversos que puedan producirse, adoptar las medidas necesarias para la protección a la salud y establecer, en su caso, un conjunto de de obligaciones a fin de reforzar las garantías sanitarias. En línea con las razones expuestas en la sentencia, la Sala considera que Real Decreto de referencia no contiene una regulación exhaustiva del derecho a la información ni puede entenderse que la disposición sobre confidencialidad que contiene sea incompatible ni limite el acceso a la información en los términos de la Ley 13/2019*".

2. REUTILIZACIÓN DE LOS DATOS DE SALUD

2.1. CONDICIONES DE REUTILIZACIÓN DE LA INFORMACIÓN

La aplicación de las TICs a la información administrativa facilita su posterior reutilización, considerándose un tratamiento de información. Así, este tratamiento, en la medida en que contenga datos personales, será aplicable la normativa sobre protección de

[715] SAN, Sala de lo Contencioso, de 18 de diciembre de 2019.

datos personales, por cuanto existe una colisión con el derecho fundamental a la protección de datos que limita la reutilización de la información; ello, sobre la base de que, en este caso, resultan aplicables los principios y derechos aplicables a todo tratamiento de datos, constituyendo una cesión de datos personales, derivados de la utilización de la información en poder de la Administración por empresas; por lo que sería necesario el consentimiento del interesado[716]; excepto si estamos ante las situaciones excepcionales previstas en el art. 6 RGPD[717].

La reutilización de la información pública[718], en el entorno del *Open data*, a nivel europeo, está regida, de una parte, por el "Libro Verde sobre la información del sector público", de 1998, cuyos conceptos y principios siguen hoy vigentes, y por la Directiva 2003/98/UE[719], la cual señala la necesidad de procesar y publicar la información en unas condiciones que faciliten la reutilización[720]:

a) Deben abrirse todos los datos de carácter público que no estén sujetos a restricciones de privacidad, seguridad o derechos de autor (públicos).

b) Deben publicarse los datos tal y como están en su origen, sin procesar y manteniendo el mayor nivel de detalle posible (datos en brutos).

c) Los datos serán precisos y actualizados.

d) Los datos deben ser accesibles para el mayor número de usuarios posible.

e) Los datos deben ser estructurados para que puedan ser puedan ser procesados de forma automática por un ordenador como garantía de su reutilización.

f) Los datos deben estar disponibles para todos, sin necesidad de identificarse

[716] Art. 11 LOPD: "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".

[717] Coincidentes, como hemos visto, con las incluidas en la LOPD y el RLOPD.

[718] Según el art. 2.4. de la Directiva 2003/98/CE, reutilización supone "(…) el uso de documentos que obran en poder de organismos del sector público por personas físicas o jurídicas con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos en la misión de servicio público para la que se produjeron. El intercambio de documentos entre organismos del sector público en el marco de sus actividades de servicio público no se considerará reutilización".

[719] Directica 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.

[720] Siguiendo a SUBIRANA DE LA CRUZ, *op.cit.*, pp. 1-14.

previamente.

g) Los formatos de los datos no deben pertenecer a una entidad o a una herramienta propietaria de una entidad (éste sería el caso de los formatos Word, Excel, etc.).

h) Los datos deben estar 100% libres de derechos, patentes, copyright y no estar sujetos a derechos de privacidad, seguridad o privilegios.

Por tanto, los datos abiertos listos para ser reutilizados no sólo tienen que se ser accesibles, sino que deben cumplir ciertas condiciones; permitiendo a ciudadanos y empresas ser partícipes con la sociedad, generando, al mismo tiempo, actividad económica mediante la creación de nuevos productos y servicios, formando parte, por ello, de la denominada "economía circular"

De la trasposición de la Directiva 2003/98/CE surgió la Ley 37/2007, sobre reutilización de la información del sector público, que supuso el inicio de una estrategia nacional en materia de datos abiertos. Así mismo, del desarrollo de esta ley surgió el Real Decreto 1495/2011, de 24 de octubre, que estableció un modelo de aviso legal para homogeneizar derechos y condiciones de reutilización. Y, a su vez, de dicho decreto, surgió la Norma Técnica de Interoperabilidad (que establece condiciones comunes para la reutilización de documentos y recursos de información, referidos en el art. 3 de la ley) y a la creación de un catálogo de información pública reutilizable.

Ante la necesidad de incorporar al Derecho interno los nuevos planteamientos de la Directiva 2013/37/CE[721] se publicó la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007[722], la cual establece la obligación inequívoca de los organismos públicos de autorizar la reutilización de los documentos, excepto los expresamente excluidos (artículo 3.3.), además de –siempre que sea posible y no sea desproporcionado- facilitar los documentos en formatos abiertos y legibles por máquina conjuntamente con sus metadatos, con el mayor grado posible de precisión y desagregación. Tanto el formato como los metadatos seguirán normas formales y estándares abiertos (art. 5.2.9).

[721] Enfocada más a los aspectos económicos de la reutilización que al acceso a la información.

[722] El Reglamento de desarrollo se ha incorporado por Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.

El surgimiento de la reutilización parte de la perspectiva de que, la abundante información en poder de la Administración, además de su indudable utilidad de desarrollo de la actividad administrativa, se considera que tienen un gran valor para ser utilizada por el sector privado empresarial impulsando la actividad económica y la creación de riqueza. En este entorno, la Directiva 2003/98/CE persigue armonizar la reutilización de la información del sector público de la UE, eliminando las barreras derivadas de un mercado europeo fragmentado.

Recientemente, el Parlamento Europeo ha aprobado la Directiva 2019/1024/UE, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización del sector público, que modifica sustancialmente la Directiva 2013/37/UE, en el sentido de acentuar la utilización de los datos abiertos y la utilización de mecanismos que aumenten el suministro de datos públicos para su reutilización por ciudadanos y personas jurídicas. Una de las principales novedades de esta directiva es la regulación de los llamados datos dinámicos a través de interfaces de programación de aplicaciones (API) y otros mecanismos para aumentar el suministro de datos públicos valiosos para su reutilización por ciudadanos y personas jurídicas.

La reutilización constituye un elemento de la transparencia relacionado con el acceso a la información pública. La propia ley destaca la importancia de la reutilización como "(…) *elemento de transparencia y guía para la participación democrática* (…)"[723]. Sin embargo, difiere de la transparencia, en cuanto que ésta tiene unos fundamentos constitucionales (derecho de participación en los asuntos públicos (art. 23 CE), la libertad de expresión y el derecho a solicitar y recibir información (art. 20 CE), que no coinciden con la finalidad comercial o económica de la reutilización, que hace que las empresas no sometan a reutilización toda la información administrativa sino únicamente aquella que tiene interés económico.

Sobre el alcance de lo que se entiende por reutilización, ésta supone "(…) *el uso de documentos que obran en poder de la Administración y organismos del sector público por personas físicas o jurídicas con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública* (…)"[724]. Así, resulta

[723] Preámbulo de la ley, coincidente con el Considerando 16 de la Directiva 2003/98/CE.
[724] Art. 3 Ley 37/2007.

necesaria la publicación de la información y datos en formatos que propicien que se generen nuevas utilidades, productos o servicios.

Las prescripciones de la ley se aplican a los documentos elaborados o custodiados por las administraciones y órganos del sector público, quedando excluidos los documentos que se relacionan en el art. 3, entre los que se encuentran: " (…) *los documentos cuyo acceso esté limitado o se haya declarado incompatible por motivo de datos personales" (j)"*; y en ningún caso, podrá ser objeto de reutilización, la información en la que la ponderación, a la que se refieren los artículos 5.3 y 15 de la LTBG, arroje como resultado la prevalencia del derecho fundamental a la protección de datos de carácter personal, a menos que se produzca la disociación de los datos a la que se refiere el artículo 15.4 de la citada Ley.

La ley 37/2007 no establece ninguna habilitación legal para la cesión de datos personales con la finalidad de reutilización de la información pública, señalando que la ley se aplicará "(…) *sin perjuicio del régimen aplicable al derecho de acceso a los documentos y a las especialidades previstas en su normativa reguladora*" (art. 1).

Además, la LTBG, incluye dentro de su contenido diversos principios y obligaciones en materia de formatos de publicación para favorecer la reutilización de la información:

"*La información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada, así como su identificación y localización*" (art. 5.4). Por otra parte, la información que se publique en el portal de transparencia deberá, además de ser accesible e interoperable, ser reutilizable, mediante formatos que lo permitan (art. 11.c).

El GT29 ha venido a señalar que la comunicación de datos personales propios de la administración a terceros solicitantes debe considerarse tratamiento de datos personales, adecuándose, necesariamente, a todas sus prescripciones, al margen del modo utilizado para difundirlos o su carácter público o privado[725].

[725] Dictamen 5/2001, relativo al Informe Especial del Defensor del Pueblo Europeo al Parlamento Europeo sobre el proyecto de Recomendación dirigido a la Comisión Europea en la reclamación 713/98/IJH, de 17

Debe tenerse en cuenta especialmente los principios de legitimación y de calidad de los datos[726], éste último, no sólo en cuanto a la reutilización de aquella información de datos necesarios y pertinentes que permitan utilizaciones posteriores, sino por la necesidad de utilización del procedimiento de disociación de la información a reutilizar, que, como sabemos, no supone un tratamiento de datos personales. De forma que, acudiendo a la técnica de anonimización de los datos, no será necesario ningún acceso a datos personales, como sucede con la información estadística, epidemiológica o de investigación.

Por último, una vez realizada la reutilización, se produce un cambio de finalidad y el cesionario de los datos se convierte en responsable del fichero resultante, estando sometido por completo a la normativa sobre protección de datos. Además, la concesión de un nuevo o adicional uso a esta información que contiene datos personales supone un nuevo tratamiento de datos. Así, los interesados, salvo que sea imposible o desproporcionado, deberán ser informados de la cesión de los datos personales, de la finalidad del fichero, de la naturaleza de los datos cedidos y del nombre y dirección del cesionario (arts. 5 y 27 LOPD); y los derechos de los titulares de los datos permanecen exigibles totalmente.

Recordar, como señalábamos antes, que la utilización por las empresas no puede tener por objeto una actividad que es propiamente administrativa pública, quedando excluido de este concepto el intercambio "(…) *de documentos entre Administraciones y organismos del sector público en el ejercicio de las funciones públicas que tengan atribuidas*" (art. 3.1.).

---

de mayo de 2001: "los datos personales contenidos en un documento oficial o en poder de una administración u organismo público conservan este carácter personal, por lo que deben protegerse de acuerdo con la legislación en materia de protección de datos, en la medida en que el tratamiento de dichos datos pertenezca al ámbito de aplicación de esta legislación". Disponible en: http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2001/wp44_es.pdf.

[726] Al que se refiere directamente la Ley 37/2007, en el art. 8 al señalar que la reutilización de la información de las Administraciones y organismos públicos puede estar sometido a que:
"a) Que el contenido de la información, incluyendo sus metadatos, no sea alterado.
b) Que no se desnaturalice el sentido de la información.
c) Que se cite la fuente.
d) Que se mencione la fecha de la última actualización.
e) Cuando la información contenga datos de carácter personal, la finalidad o finalidades concretas para las que es posible la reutilización futura de los datos.
f) Cuando la información, aun siendo facilitada de forma disociada, contuviera elementos suficientes que pudieran permitir la identificación de los interesados en el proceso de reutilización, la prohibición de revertir el procedimiento de disociación mediante la adición de nuevos datos obtenidos de otras fuentes".

2.2. OPEN DATA Y REUTILIZACIÓN DE DATOS DE SALUD

Tratándose de datos de salud (y, en general, de datos especialmente protegidos), habrá que remitirse a lo ya visto con ocasión del examen de estos datos en el apartado específico de acceso a la información pública. Así, el régimen de prohibición estricto de los datos de salud, y en general, de los datos especialmente protegidos, han dificultado la posibilidad de su tratamiento y, en mayor medida, cuando este se realiza por entidades privadas; haciendo, por tanto, muy complicada la reutilización de estos datos.

Sin embargo, el proceso aperturista de datos está calando hondamente -aunque muy lentamente- en las AAPP; no sólo en cuanto a la reutilización y apertura de datos o la generalización de las *wearables*[727] y las aplicaciones sobre salud y bienestar, sino también por la irrupción de herramientas de realidad virtual, inteligencia artificial y técnicas de *big data* sanitario[728]; por lo que, sin duda, nos movemos en un nuevo escenario de transformación digital en el ámbito sanitario, condicionado por las herramientas tecnológicas.

En relación con la salud, en la Estrategia para el Mercado Común Digital se encuadran diversas estrategias, como la "Comunicación relativa a la transformación digital de la sanidad y los servicios asistenciales en el Mercado Único Digital y la capacitación de los ciudadanos y la creación de una sociedad más saludable", la cual puso de manifiesto la evidencia de una problemática generalizada relativa a:

a) La falta de armonización en el proceso de recopilación de los datos sanitarios, que impide realizar estadísticas y estudios comparados, incluso dentro de los hospitales de un mismo país.

b) Falta de homogeneidad en los estándares y formatos de las historias clínicas, que impiden la interoperabilidad de los sistemas y el traslado de historias cínicas electrónicas a otros centros sanitarios,

[727] Se refiere a la información de la que disponen las empresas privadas con una finalidad comercial.
[728] ANDREU MARTÍNEZ, M, "Open data en el ámbito sanitario y su compatibilidad con la privacidad del paciente", Accueil -Les Éditions de L,IMODEV, vol 5, 2017, pp. 1-12.

c) El nivel de acceso a datos incluidos en registros de pacientes y de enfermedades es muy reducido.

A la vista de la existencia de estas barreras que dificultan la reutilización de la información sanitaria, el Consejo de Europa planteó a los estados miembros diversas propuestas: promover la utilización de sistemas interoperables; promover la utilización de estándares internacionales y abiertos, así como de estructuras de datos, sistemas de codificación y terminologías comunes que faciliten la interoperabilidad; y, por último, la creación de redes de datos y plataformas comunes descentralizadas que permitan la integración de datos en entornos seguros.

En el ámbito de la Estrategia para el Mercado Común Digital, tanto por la Comisión, como por el Parlamento, o, por ambos conjuntamente, se han presentado distintas iniciativas[729]:

- Así, en enero de 2018, la Comisión presentó una estrategia sobre una inteligencia artificial para Europa y acordó un plan coordinado con los Estados miembros.

- En abril de 2019, el Grupo de expertos de alto nivel sobre la IA presentó sus directrices éticas para una IA fiable.

- En febrero de 2020, la Comisión presentó su Libro Blanco sobre la inteligencia artificial – Un enfoque europeo orientado a la excelencia y la confianza y unas Comunicaciones tituladas «Modelar el futuro digital de Europa» y «Una Estrategia Europea de Datos».

- En relación con el Parlamento:

- El 11 de diciembre de 2012, el Parlamento aprobó dos Resoluciones no legislativas relativas al mercado interior, una sobre la culminación del Mercado

[729] Fichas temáticas sobre la Unión Europea, Parlamento europeo: https://www.europarl.europa.eu/factsheets/es/sheet/43/el-mercado-unico-digital-omnipresente.

Único Digital y otra sobre una Estrategia de libertad digital en la política exterior de la UE.

- El 4 de julio de 2013, el Parlamento aprobó una nueva Resolución sobre la culminación del mercado único digital que se centraba en la liberación del pleno potencial del mercado único digital; el cierre de la brecha de pericias; el aumento de la confianza, la seguridad y la tranquilidad de los consumidores; la creación de una oferta atractiva legal de contenido digital; el despliegue de los servicios de movilidad; y la dimensión internacional.

- En respuesta a la Estrategia para el Mercado Único Digital, el 19 de enero de 2016 el Parlamento aprobó una Resolución titulada «Hacia un Acta del Mercado Único Digital»[730].

Además, el Parlamento está construyendo el mercado único digital a través de una actividad legislativa intensiva[731].

El 20 de junio de 2019 el Parlamento Europeo y el Consejo adoptaron el Reglamento (UE) 2019/1150 sobre el fomento de la equidad y la transparencia para las empresas que utilizan servicios de intermediación en línea.

[730] En ella se solicita a la Comisión:
"que ponga fin a las prácticas de bloqueo geográfico injustificadas, mejore el acceso de los consumidores de la Unión a los bienes y los servicios, garantice un nivel de protección del consumidor equivalente y preparado para el futuro, con independencia de si se adquieren contenidos digitales en línea o fuera de línea, busque soluciones innovadoras para la paquetería transfronteriza a fin de mejorar los servicios y reducir los costes, elimine las barreras para las pymes, las empresas de nueva creación y las empresas en fase de expansión y aproveche las oportunidades que brindan las nuevas tecnologías de la información y la comunicación".

[731] Como la siguiente:
"La introducción de garantías de la neutralidad de la red; la eliminación de las tarifas de itinerancia el 15 de junio de 2017; la prohibición de prácticas de bloqueo geográfico injustificadas; la introducción de un portal digital único; y la adopción de la Directiva relativa a medidas para reducir el coste del despliegue de las redes de comunicaciones electrónicas de alta velocidad; el Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior; la Directiva sobre normas europeas de ciberseguridad; la Directiva relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales; y la Directiva sobre los derechos de autor y derechos afines en el mercado único digital.
El 18 de diciembre de 2019, el Parlamento aprobó una Resolución sobre la consecución de la transformación digital de la sanidad y los servicios asistenciales en el Mercado Único Digital, la capacitación de los ciudadanos y la creación de una sociedad más saludable y está elaborando actualmente un informe de iniciativa legislativa sobre una Ley de servicios digitales: una mejora del funcionamiento del mercado único".
Fichas temáticas sobre la Unión Europea, Parlamento europeo:
https://www.europarl.europa.eu/factsheets/es/sheet/43/el-mercado-unico-digital-omnipresente.

Destacamos, por su incidencia en el ámbito de la Salud Pública, y en concreto sobre el COVID-19, la Recomendación de la Comisión, de 8 de abril de 2020, relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados[732].

Tratándose de datos de investigación en salud, la Directiva 2019/1024/UE, insta a que los datos derivados de investigaciones realizadas con fondos públicos sean totalmente accesibles, aplicando el principio de apertura por defecto y de compatibilidad con los principios FAIR (*findable, accesible, interoperable and reusable*). Entre las redes de datos de investigación financiadas por la UE destacan: FAIRplus, FAIRsFAIR y FAIR4Healt; ésta es una red liderada por el Servicio Andaluz de Salud, a través de: *Orphanet*, que es un portal de enfermedades raras que dispone de un directorio de laboratorios, de ensayos clínicos y de profesionales sanitarios; y *Orphadata*, que es un portal de datos de investigación sobre enfermedades para su reutilización por ciudadanos e investigadores clínicos[733].

Los beneficios para el ámbito de la salud que puede aportar el *open data* y la reutilización de la información pueden sintetizarse de la siguiente forma:

a) los que afectan a los gobiernos, al permitir una mejora de la toma de decisiones en salud, incrementando la eficiencia y la transparencia de los servicios públicos sanitarios;

y, b) en cuanto a los datos, al poder recibir más y mejor información, permite una mayor implicación en sus procesos de salud con un mejor resultado, lo que se traduce en un paciente más responsable y participativo en las decisiones de salud que le afectan ("empoderamiento del paciente").

[732] Accesible en: file:///C:/Users/Usuario/Downloads/ES_ACTpdf.pdf.

[733] *The conversation*, "Por qué es tan difícil reutilizar nuestros datos de salud en investigación", disponible en: https://theconversation.com/por-que-es-tan-dificil-reutilizar-nuestros-datos-de-salud-en-investigacion-113092

En España, son los Servicios regionales públicos de Salud los que mayor volumen de datos de salud generan (no sólo asistenciales, sino financieros, sobre personal, estadísticas, etc.), aunque también los provenientes del sector de colaboración público-privado y proveedores sanitarios (como la industria farmacéutica) generan cada vez más cantidad de información; sin olvidar la generada por los dispositivos móviles y las aplicaciones sobre salud y bienestar, además de las *wearables*.

La utilización de técnicas de *big data*[734] o macrodatos, que contiene un gran potencial del que pueden plantearse modelos predictivos, que faciliten la investigación y el desarrollo en el ámbito de la salud, así como de inteligencia artificial (la cual precisa datos masivos que han de ser accesibles en condiciones óptimas para su tratamiento automatizado, a fin de modelizar el comportamiento humano en términos computacionales), permiten la realización de tratamientos masivos de datos con un gran potencial de información a aplicar al propio paciente o al conjunto del sistema sanitarios (planificación y estadísticas).

Sin embargo, aunque permiten valorar y comparar la eficacia del tratamiento que se presta en el conjunto de los servicios sanitarios, cuando se necesita utilizar los datos para utilizarlos en un tratamiento de un paciente concreto surgen los problemas jurídicos, ya que la finalidad curativa necesita un seguimiento personalizado, que en último caso implica contrastar la información obtenida con los datos de salud del paciente; proceso personalizado, en el que deben respetarse sus garantías de confidencialidad y, por tanto, al margen de la utilización de herramientas técnicas.

No obstante, si analizamos qué información sanitaria se encuentra actualmente estructurada, España todavía tiene mucho trabajo que realizar para alcanzar al Reino Unido, que es el país que se sitúa a la cabeza; aunque se están realizando avances en telemedicina y en los sistemas de historias clínicas y recetas electrónicas.

[734] Se definen por GARTNER como "los activos de información caracterizados por su alto volumen de velocidad y variedad que demandan fórmulas innovadoras y rentables de procesamiento de información para mejorar la comprensión y toma de decisiones", disponible en: https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/#5a57875342f6

Así, se han señalado (por el NHS inglés) los siguientes obstáculos que impiden una mayor disponibilidad de los datos de salud:

-las barreras institucionales, burocráticas y culturales a la apertura de datos, que, por ejemplo, en España, se traducen en una escasa y retardada cultura del derecho a la información pública (así la LTBG ha sido una norma retardada respecto a la generalidad de las normas europeas).

-la protección de la privacidad, al tratarse del manejo de datos sensibles, en el cual, incluso utilizando técnicas de anonimización, no puede asegurarse totalmente la no reidentificación, así como el riesgo derivado del empleo de técnicas de *big data*[735].

-los obstáculos derivados de los estándares técnicos y de los problemas de interoperabilidad, denominada "liquidez de los datos", para determinar la capacidad de los datos de fluir con facilidad entre todos los agentes intervinientes en el ámbito sanitario[736].

Actualmente el Sistema Nacional de Salud se encuentra ante la necesidad de afrontar retos importantes, como los siguientes[737]:

- Envejecimiento de la población. Ante la previsión futura de una mayor población cada vez más envejecida y cronificada, lo que va a suponer una mayor demanda de recursos económicos.
- Mayor inversión en investigación y fomento de la reutilización de datos.
- Necesidad de promover una mayor eficacia en la gestión sanitaria.
- Desequilibrios en el acceso al SNS.
- Baja eficiencia en los costes de los servicios.
- Necesidad de mejorar la rendición de cuentas y el control.
- Escasa personalización y proactividad.

[735] Resaltar la realidad del proyecto *Hikari*, que todavía está en fase de pruebas, basado en la aplicación de técnicas de *big data* al ámbito de la salud mental, en concreto para el estudio de los casos de suicidio.
[736] ANDREU MARTÍNEZ, *op.cit.*, pp. 1-12.
[737] Fuente: Ministerio de Sanidad, Consumo y Bienestar Social.

- Falta de interoperabilidad de los sistemas. Así, un gran problema es la falta de interoperabilidad de los sistemas informáticos de gestión de sanitaria, no sólo a nivel de interconexiones entre los distintos Servicios Regionales de Salud entre sí y con el Ministerio de Sanidad, sino que dentro de los propios sistemas internos de cada Servicio Regional de Salud.
- Escaso impulso del Gobierno abierto: transparencia, participación y colaboración.

Así, nuestro sistema sanitario necesita superar estos retos mediante la transformación digital y la apertura de datos, derivada de la gestión sanitaria tanto pública como privada; de forma que se lleve a cabo una transformación radical en el ámbito de la gestión de la actividad sanitaria y, sobre todo, en la prestación de servicios sanitarios y complementarios.

2.3. HERRAMIENTAS TECNOLÓGICAS PARA EL TRATAMIENTO DE LA INFORMACIÓN EN EL ÁMBITO DE LA SALUD

Las llamadas TICs, en la actualidad, se caracterizan por la movilidad y ubicuidad de los dispositivos y la interconexión con otros sistemas redes mediante telefonía móvil o internet; de forma que la emisión de datos del paciente -disociados- se obtienen sin la presencia física del paciente en el centro sanitario, pudiéndose agregar de forma instantánea al conjunto de datos de ese paciente[738].

Así, el estado actual de creciente modernización tecnológica se caracteriza por un impulso generalizado de la utilización de medios electrónicos en la gestión sanitaria: bien, a través de tarjetas inteligentes que incorporan datos básicos del paciente, como medio identificativo del paciente-usuario de los servicios de salud; también, el acceso a los datos de información del paciente contenidos en la HC electrónica, a través de distintos tipos de dispositivos; permitiendo una mayor accesibilidad y facilidad para otras utilidades, tanto en beneficio directo del paciente como desde el punto de vista de la investigación;

[738] *Iniciativa Aporta*, Gobierno de España, red.es, "Datos abiertos y sanidad: contexto tecnológico, actores implicados y marco jurídico", diciembre 2019, pp. 1-48.

y por último, la receta electrónica, que, aparte de su comodidad para el conjunto médico-paciente-boticario, aporta nuevas posibilidades para la racionalización y el control del gasto sanitario.

Diversas disfuncionalidades del SNS, como señalábamos, pueden y deben ser afrontadas desde la aplicación de las nuevas tecnologías, facilitando una mayor interconexión de los sistemas de información para permitir un mejor acceso a los datos de salud y su actualización inmediata a las variaciones del estado de salud del paciente; lo que puede realizarse de forma automatizada empleando medios telemáticos, incluso a través de interconexiones directas entre los propios dispositivos y los objetos, conforme al denominado modelo de Internet de las Cosas (IoT). Otros dispositivos y aplicaciones médicas innovadores utilizados en la prestación de servicios sanitarios sería el "Internet of Medical Things" (IoMT)[739], que se conectan a sistemas TI (Tecnología de la información) de atención médica a través de redes informáticas en línea, permitiendo recoger y tratar casi de forma instantánea datos de salud del paciente.

Por tanto, la utilización de las TICs por las Administraciones públicas sanitarias supone un requerimiento fundamental que permite la reutilización de la información a través del tratamiento de datos automatizado, siguiendo los estándares reconocidos de buenas prácticas, en la medida que están obligadas por las normas de procedimiento administrativo común y régimen jurídico del sector público a acomodarse a las normas y criterios sobre interoperatividad.

Resulta interesante traer a colación la posición de la AEPD[740] sobre el tema de la reutilización de datos de salud, basada en promover una mayor utilización y reutilización de los datos sanitarios, minimizando los riesgos. Así, partiendo de las orientaciones del GT29, se decanta por la anonimización para compatibilizar los dos derechos afectados, aunque considerando lo sensible de la materia sanitaria; por lo que debe perseguirse que

[739] Pueden aportarse diversos ejemplos del uso del *IoMT*: Dispositivos portátiles *mHealth* de los pacientes, que envían información para la monitorización remota de pacientes; sensores que permiten el seguimiento de pedidos de medicamentos; las bombas de infusión que se conectan a paneles analíticos, y camas de hospital dotadas de sensores que miden los signos vitales de los pacientes. Fuente: https://internetofthingsagenda.techtarget.com/

[740] Documentos de la AEP: "Orientaciones sobre protección de datos en la reutilización de la información del sector público", de 13 de octubre de 2016, disponible en: https://datos.gob.es/es/documentacion/orientaciones-sobre-la-proteccion-de-datos-en-la-reutilizacion-de-la-informacion-del, y "Orientaciones y garantías en los procedimientos de anonimización de datos personales"

la disociación sea irreversible, lo que, como hemos indicado con ocasión de los datos incluidos en la investigación biomédica, parece muy difícil de asegurar.

De ahí, que una alternativa es la realización de una evaluación de riesgos de la reidentificación, además de la posibilidad de añadir garantías jurídicas adicionales, como la prohibición expresa de la reidentificación y/o de utilizar datos para elaborar perfiles.

Con ocasión de la investigación de datos de salud, se plantea el alcance de, hasta qué punto, los pacientes, cuyos datos son utilizados en beneficio de la ciencia y la investigación, pueden permitir esta utilización sin su consentimiento, aunque se trate de una base legítima legal de tratamiento; señalándose que, frente a la opción del consentimiento del afectado, puede incrementarse la información sobre el uso de sus datos personales anonimizados, y de que, aunque no puede garantizarse su anonimización total, si puede garantizarse que no se explotarán de forma privada para finalidades distintas de la investigación.

2.4. REUTILIZACIÓN Y PROTECCIÓN DE DATOS PERSONALES

El mayor manejo de la información deriva de una mayor presencia en la gestión sanitaria de herramientas tecnológicas; sin embargo, tiene como contrapartida un mayor riesgo para proteger la privacidad (a mayor tecnificación mayor vulnerabilidad), que como hemos visto, el nuevo RGPD aborda atribuyendo al responsable del tratamiento un papel proactivo en el aspecto de la seguridad los datos, a través de las evaluaciones de impacto y análisis de riesgo, y con especial atención en la reidentificación; lo cual tiene incidencia en el acceso a la información sanitaria, y, en concreto, en relación con la reutilización posterior de esa información para finalidades distintas de las que justificaron el tratamiento inicial de datos. De forma que el paciente o usuario de la salud dispone de los principios y la normativa sobre protección de datos como garantía de su posición jurídica, en la medida en que de ella derivan los límites, garantías y condiciones necesarios para la reutilización de la información sanitaria.

Por ello, al margen del cumplimiento de las limitadas finalidades que justifican el acceso a estos datos, no debería accederse a una reutilización de datos sanitarios si previamente no se han respetado las normas de seguridad y de anonimización de datos; y, si los datos

sanitarios fueran de personas identificables, su utilización únicamente sería posible desde el respeto a los límites de la información, reforzándose la posición del consentimiento informado.

Dentro del ámbito normativo del acceso y la reutilización de la información pública vemos como existe una tensión latente entre dos posiciones: de una parte, una concepción legal de la gestión de la información, preocupada básicamente por la posición jurídica de las personas que son titulares de datos; y de otro lado, la existencia de un interés público en que los datos generados puedan ser cedidos a terceros con fines de reutilización. Y esta tensión aparece incrementada cuando existe la reutilización de datos conforme a los criterios de datos abiertos, por cuanto el tratamiento automatizado afecta en mayor grado al derecho a la protección de datos y los datos van a utilizarse (tratarse) con otra finalidad distinta de la inicial; de ahí que sea necesaria la prestación del consentimiento del titular afectado, lo que puede constituir un obstáculo a la reutilización, por lo que el Reglamento se decanta por la utilización de la anonimización, aunque ello comporta mayores costes empresariales al requerir una reelaboración de la información (salvo que se haya aplicado técnicas de privacidad por el diseño)[741].

En relación con la investigación en salud pública y biomédica, como hemos visto, la LOPDGDD, en su Disp.Adic. 17ª exige la seudonimización de los datos (siendo aplicable la normativa sobre protección de datos), aunque no se contempla su aplicación con carácter general en la utilización de datos abiertos objeto de reutilización, prevista por la normativa de ésta última. Por ello, sólo procedería la apertura de datos si existe consentimiento del titular o bien se conceda un acceso anonimizado de los datos, aunque debería asegurarse la no reidentificación del titular, lo que constituye una importante dificultad para los datos de salud.

Recordemos la prohibición de revertir el proceso de disociación a través de la incorporación de nuevos datos procedentes de otras fuentes, en los casos en que la información (que puede estar disociada) contenga elementos que permitan la identificación del titular en el proceso de reutilización[742].

[741] Iniciativa Aporta. *Op.cit*.
[742] ANDREU MARTÍNEZ, B., *El acceso a la información*, *op.cit*., pp. 6 y ss.

Además de la seudonimización, resulta necesario el cumplimiento de una serie de requisitos necesarios para que el tratamiento de la información sea lícito:

-Que exista una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización, y conserven la información que posibilite la reidentificación.

-Que los datos se sometan al examen previo de un comité de ética de la investigación.

-Que se adopten medidas de seguridad específicas paras evitar la reidentificación y el acceso de terceras partes no autorizadas.

-Que por parte del equipo investigador exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

CAPÍTULO III

EL DERECHO A LA PROTECCIÓN DE DATOS Y EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA SANITARIAS

1. PRESUPUESTOS PARA LA APLICACIÓN DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS

1.1. RELACIONES ENTRE AMBOS DERECHOS

La existencia del Estado Democrático de Derecho reclama la coexistencia armonizada y equilibrada de los distintos derechos constitucionales en juego, de manera que no se produzcan perjuicios y desequilibrios derivados de la imposición de unos derechos sobre los otros, salvo la existencia de causas realmente justificadas. En todo caso, deben evitarse la producción de estos mínimos quebrantos para los titulares de estos derechos. Así, podemos hacer referencia a la interacción entre la libertad de expresión con los derechos a la intimidad y al honor, frecuentemente objeto de confrontación. De esta forma, las relaciones entre el derecho a la protección de datos y el derecho de acceso a la información pública deberían ser subsidiarios de estos principios[743].

En todo caso, es preciso aclarar el ámbito de relaciones entre ambos derechos, habida cuenta de la trascendencia de la transparencia como elemento básico de una sociedad democrática y abierta; sin que el derecho a la protección de datos deba suponer un obstáculo al acceso a la información; aunque, no obstante, debe considerarse su presencia

[743] Ya hemos visto anteriormente como TRONCOSO REIGADA, A., *Transparencia administrativa y protección de datos personales…*, se refería a la necesidad de contar con el equilibrio y proporcionalidad en las relaciones de los derechos fundamentales con otros derechos. En el mismo sentido, GUICHOT, E., *Publicidad y privacidad de la información administrativa*, Thomson Reuters y AGPDCM, Madrid, 2008.

como elemento excepcional a considerar junto con la protección de la intimidad, entre otras excepciones[744].

Las relaciones entre ambos derechos en confrontación deben resolverse consiguiendo un equilibrio en la aplicación de estos[745]. En este contexto, y a efecto de analizar las relaciones en conflicto, resultan fundamentales los principios de las SSTJUE: asunto *Rundfunk* y otros[746], cuyos principios son determinantes en la definición de los principios de finalidad y proporcionalidad en su aplicación para buscar un equilibrio en la aplicación de los derechos de acceso a la información y de protección de datos; y *Bavarian Lager contra Comisión*[747], por la que se concluye que "(…) el mero hecho de que un documento contenga datos personales no significa necesariamente que se ponga en peligro la intimidad o la integridad de las personas de que se trata, a pesar de que la actividad profesional no esté, en principio, excluida del concepto de "vida privada" en el sentido del art. 8 CEDH".

En concreto, sigue señalando el tribunal, contener los nombres de los representantes de las entidades (que figuran en la reunión de la Comisión, que han sido solicitados) que participaron en la reunión no pone en peligro la intimidad de las personas, ya que éstas actúan en representación de sus entidades y sus opiniones son imputables a dichas entidades. Este asunto, como hemos visto, se contempla desde el Reglamento 1049/2001, que contiene, como excepción al principio de apertura y el derecho de acceso, la existencia de datos personales que puedan suponer un perjuicio para la protección de la intimidad y la integridad de las personas.

En este sentido, en la sentencia del TSJUE, el Abogado General Sharpston en sus Conclusiones de 15 de octubre de 2009, en el caso Comisión Europea vs *The Bavarian Lager Co. Ltd*, señala: "(…) dado que los dos derechos fundamentales (acceso a los documentos y protección de los datos personales) de que se trata tienen el mismo rango,

744 PIÑAR MAÑAS, J.L., *Transparencia, acceso a la información y protección de datos*, *op.cit*., pp. 51-54.
745 TRONCOSO REIGADA, A., *Transparencia administrativa y protección de datos personales…, op.cit*., pp. 43 y ss.
746 STJUE de 20 de mayo de 2003, asunto *Rundfunk* y otros, C-465/00.
747 STJUE, de 8 de noviembre de 2007, *Bavarian Lager contra Comisión*

no puede darse una solución al conflicto que ignore uno de ellos y de prioridad absoluta al otro. Así mismo, el Tribunal de Justicia, ha señalado que, en circunstancias de colisión de los derechos fundamentales, han de ponderarse los intereses enfrentados buscando un justo equilibrio entre esos intereses y los derechos fundamentales en juego"[748].

Por tanto, el principio que sienta esta sentencia supone que, si se va a enjuiciar una solicitud de acceso a información que contenga datos personales de un tercero, resulta de aplicación la normativa reguladora del derecho de acceso, no la de la protección de datos; que, no obstante, excepciona el principio de acceso cuando se puedan producir perjuicios efectivos al derecho a la intimidad (incluiría los datos especialmente protegidos o sensibles).

El GT29, se refiere a la necesidad de conciliar el respeto del derecho a la intimidad y a la protección de datos personales con el derecho al acceso a la información pública, considerando los siguientes aspectos:

a) Valoración caso por caso del caso concreto, examinando si un dato de carácter personal puede publicarse o ser accesible y, si es afirmativo, en qué condiciones y en qué soporte.

b) Principios de finalidad y legitimidad.

c) Información de la persona en cuestión.

d) Derecho de oposición del afectado; utilización de las nuevas tecnologías para un mayor respeto del derecho a la intimidad[749].

Con anterioridad a la publicación de la LTBG, asistíamos a una jurisprudencia muy escasa y poco elaborada que relacionaba el acceso a la información pública y la intimidad. En este sentido, la STC 144/1999, de 22 de julio, dictada en relación con el acceso a datos "materialmente íntimos", como son los relativos a condenas penales que figuran en el

[748] Sentencia del Tribunal de Justicia (Gran Sala) de 29 de junio de 2010, considerando 95. Esta sentencia anula la STJUE, asunto T/194/04, *Bavarian Lager contra Comisión.*

[749] GT29 Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, adoptadas el 29 de noviembre de 2017.

Registro Central de Penados y Rebeldes, pese a que no establece una doctrina general sobre el acceso, si señala un conjunto de principios de gran importancia en la aplicación de las relaciones entre el derecho de acceso y el de protección de datos personales[750].

Llegados a la actual regulación del RGPD, vemos como sí se aborda la relación entre ambos derechos. Así, de una parte, el art. 86[751] contempla la necesidad de conciliación de los dos derechos conforme a lo previsto en el Reglamento, en el supuesto de acceso a documentos oficiales; y de otra, resulta necesario tener en cuenta lo dispuesto en el Considerando 154, que considera de interés público el acceso a documentos oficiales[752].

---

[750] Principios que, como señala GUICHOT REINA, E., en *Comentario a la ley Orgánica de Protección de Datos Personales*, *op.cit*., pueden sintetizarse del siguiente modo:
"(…) el artículo 18.1 CE no garantiza el secreto incondicionadamente, pero sí impone que se establezcan las debidas garantías, en especial, cuando la protección de otros derechos fundamentales o bienes constitucionalmente protegidos pueden justificar que ciertas informaciones relativas a una persona o su familia sean registradas y archivadas por un poder público. 2) La garantía de la intimidad de los datos personales en poder de la Administración, constitucionalmente garantizada en el artículo 18.1 CE, tiene su acogida legal tanto en el artículo 37 LPC como en la normativa sobre protección de datos. 3) El acceso por terceros a información personal en poder de la Administración ha de tener cobertura legal y sólo está justificado si responde a alguna de las finalidades que explican la existencia del Archivo o Registro en el que estén contenidas; fines que deberán coincidir con alguna de las limitaciones constitucionalmente impuestas a la esfera íntima del individuo y su familia. 4) Es el legislador el que debe establecer en cada caso en qué casos cabe el acceso por terceros de datos íntimos de un ciudadano y en qué términos puede llevarse a cabo. Corresponde al titular del fichero adoptar todas las medidas oportunas para garantizar esta correspondencia. En este mismo sentido parece apuntar la jurisprudencia del Tribunal Supremo, que conforme a los principios de adecuación y finalidad, ha declarado ilegal la publicación íntegra de sentencias que incluya datos personales, cuando no es necesaria para conseguir la finalidad de publicidad buscada por el Registro en cuestión (es el caso de la STS de 12 de febrero de 2002 [RJ 2002, 3329], que analiza del artículo 21.1 del RD 1828/1999, de 3 de diciembre, que regula el Registro General de Condiciones Generales de la Contratación)".

[751] "Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento".

[752] "El presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. 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, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento. La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos. La Directiva 2003/98/CE del Parlamento Europeo y del Consejo no altera ni afecta en modo alguno al nivel de protección de las personas físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida

El término "documentos oficiales" no debe entenderse en su sentido estricto de certificación de carácter oficial, sino que debe ir en un sentido más amplio, incluso que el sentido de "documento público" acuñado por la LPAC; ya que, hablando en los términos de la LTBG, el objeto de la información solicitada se refiere a "contenidos o documentos, cualquiera que sea su soporte" que obre en poder de los sujetos obligados y que hayan sido elaborados o adquiridos por éstos en el ejercicio de sus funciones (art. 13).

Del mismo modo, el sintagma "acceso del público" no plantea ninguna duda sobre su referencia a cualquier persona que solicite información pública en los términos del art. 17.1 de la LTBG[753].

De esta forma, este carácter expansivo del contenido de la información a suministrar hace que únicamente pueda denegarse el acceso cuando se trate de información de carácter auxiliar o de apoyo, o bien que concurra alguno de los demás límites (art. 14.1) o causas de inadmisión (art. 18.1) previstos en dicha ley.

Por tanto, de la aplicación conjunta de ambos preceptos resulta:

a) que se reconozca expresamente la posibilidad de comunicación o acceso a documentos públicos que contienen datos personales, limitando que puedan imponerse exclusiones absolutas por la normativa sobre protección de datos;

b) que uno de los elementos de la ponderación en la aplicación de ambos derechos consistirá en la conciliación de los mismos;

y, c) que en dicha ponderación se debe tener en cuenta la consideración de interés público (y, por tanto, legítimo) del derecho de acceso, lo que presupone un interés legítimo al acceso, sin que deba prevalecer este derecho en todo caso.

Si examinamos el ámbito de aplicación de la normativa de protección de datos y la LTBG, vemos como hay una relación entre ambas: convergen ampliamente en el punto en el que la información pública contiene datos personales de todo tipo, según el tipo de

por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales".

[753] ENÉRIZ OLAECHEA, J., *op.cit.*, pp. 6 y ss.

información. Así, la relativa a la protección de datos (art. 2 RGPD), se aplica a cualquier tratamiento, tanto del sector público como del sector privado, 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, excluyendo los tratamientos, previstos en el art. 2.2. del RGPD, de los de personas fallecidas y los sometidos a protección de materias clasificadas. Por su parte, la LTBG se aplica a todo el sector público (art. 2.1.) y a una parte del sector privado vinculado al público (art. 4.1.).

Resulta muy interesante acudir por su trascendencia al contenido del informe de la AEPD de 5 de junio de 2012, en el que se destaca la necesidad de que la transparencia sea "(…) congruente con los principios que conforman el derecho fundamental a la protección de datos de carácter personal (…)"; de forma que la comunicación de la información por parte de los sujetos públicos supondrá un tratamiento específico de los datos personales incluidos en ella. Y si el acceso se realizara sobre un fichero de datos de carácter personal, conforme a LOPD, deberán considerarse las previsiones de esta ley, de forma que para la concesión de la comunicación será necesaria que ésta sea conforme a la LTBG y a la LOPD.

Como señala FERNÁNDEZ RAMOS[754], con la entrada en vigor de la LTBG se ha puesto fin de alguna forma al desequilibrio marcado existente entre transparencia pública y protección de datos. Sin embargo, en la medida que se considera como cesión o comunicación de datos cualquier acceso por parte de terceros a datos personales en poder de las AAPP (en la que con carácter general se exige el consentimiento del interesado (art. 6 RGPD) y, dado que la propia legislación de protección de datos no hace discriminación entre datos públicos y privados, se está produciendo un evidente desequilibrio y vulneración del principio de proporcionalidad, al supeditarse el derecho de acceso al derecho a la protección de datos.

De esta forma, vemos que ha venido existiendo una cierta laguna regulatoria por parte de la normativa de acceso a la información pública, que a la Administración le sirve de mucha utilidad, por cuanto le permite interpretar ampliamente (por supuesto en favor de la denegación) los casos de admisión de solicitudes de acceso a la información pública

[754] FERNÁNDEZ RAMOS, S., *Acceso a la información pública versus protección de datos personales*, *op.cit*., pp. 1-5

apelando a la existencia de datos personales que justifiquen la denegación[755]. De ahí, que el recurso a la existencia de datos personales sea prácticamente la causa más importante en las denegaciones de acceso a la información pública[756]; por lo que, puede concluirse, que el derecho de acceso tendrá mayor o menor efectividad en función de cómo se articule por la Administración esta invocación a los datos personales.

Así, ante la existencia de esta problemática, la LTBG ha venido a completar esta laguna legal colmada, hasta entonces, por la legislación de protección de datos, entrando a regular un artículo dedicado específicamente a la protección de datos personales que, como señala Fernández Ramos[757], respondía inicialmente a la propuesta de la AEPD, aunque luego se modificó tras el informe del Consejo de Estado.

1.2. PRESUPUESTOS PARA LA APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS. CONSIDERACIONES SOBRE LOS DATOS DE SALUD

El derecho de protección de datos no solamente implica la existencia de instrumentos legales que permiten al titular de los datos gozar de una autentica disposición de su información personal, con la exigencia de manifestar su consentimiento previo al uso de sus datos personales; también conlleva el hecho de ser informado sobre el destino que le darán, acceder a los contenidos que los incluyan, rectificación y hasta eliminación a solicitud del interesado. Sin embargo, los datos de carácter personal sobrepasan el ámbito del derecho a la intimidad y se exponen a la pérdida o afectación por el uso generalizado

[755] En la comparecencia del Director de la AEPD, Comisiones, nº 248, de 23 de enero de 2013, p.4, señalaba que "la Ley de Transparencia pondrá término a una práctica relativamente frecuente, consistente en invocar indebidamente, sin fundamento y sin consultar a la agencia de protección de datos para denegar el acceso a determinadas informaciones, lo cual ha contribuido a generar en la opinión pública una errónea percepción de que la protección de datos constituye un obstáculo a la transparencia".

[756] Así lo señalaba el Sindic de Greuges de Cataluña, "El derecho de acceso a la información pública", Informe extraordinario, marzo 2012, p.17.

[757] FERNÁNDEZ RAMOS, S., *Acceso a la información pública versus protección de datos personales*, *op.cit*., pp. 1-5.

de productos y servicios[758], gracias a los avances tecnológicos, en especial los relacionados a la difusión a través de la web[759].

Previamente a entrar examinar el "juego" de relaciones entre la LTBG y la normativa de protección de datos, se ha de determinar cuando entra en aplicación la propia normativa de protección de datos, para lo que es necesario que la información que se vaya a solicitar incluya datos de carácter personal; es decir: a) que encaje dentro de lo que se consideran como tales[760]; de forma que se incluyen todos los que lleven a la identificación de una persona o a su posible identificación sin que sean necesarios esfuerzos desproporcionados; sin que, por tanto, sea necesario una coincidencia entre el dato y su atribución a una persona determinada[761]; y, b) que se trate de datos personales que son objeto de tratamiento, automatizado o manual; por cuanto si no hay tratamiento no puede hablarse de cesión de datos, en cuyo caso estaríamos ante la afectación de otro derecho como la intimidad, pero no a la protección de datos[762].

Sin embargo, "(…) el sólo hecho de que se detecte en la documentación solicitada un dato que haga identificable a una persona física no puede conducir sin más a considerar que su divulgación entrañe una vulneración del derecho a la protección de datos personales y, en consecuencia, a que deba denegarse necesariamente el acceso a la misma. La posibilidad de que se pueda identificar a una persona física es condición *sine qua non* para que llegue siquiera a plantearse la colisión entre ambos derechos. Si no hay persona

[758] MINERO ALEXANDRE, G.,"Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario Jurídico y Económico Escurialense*, nº 50, 2017, p. 17.

[759] AEPD, Memoria 2014 publicada por la AEPD con fecha de 30 de junio de 2015. La Autoridad española de protección de datos resalta la importancia de la doctrina jurisprudencial que deja la sentencia del Tribunal de Justicia dela Unión Europea de 13 de mayo de 2014 (asunto *Google Spain y Google Inc contra AEPD y Mario Costeja*) y manifiesta su conformidad al comprobar que su labor, anterior a la decisión, como prueban sus resoluciones acerca del tratamiento de datos en los buscadores de Internet, coincide con el contenido y propósito de la sentencia. Disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/.

[760] Definiciones legales incluidas en el Reglamento Europeo de Protección de Datos personales. El artículo define los datos personales como *"*toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*"* (art. 4).

[761] SSAN de 8 de marzo de 2002 y 3 de marzo de 2014, entre otras, en las que haciendo alusión al Considerando 26 de la Directiva 95/46 CE, señala que, para determinar si una persona es identificable, hay que considerar el conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar dicha persona.

[762] TRONCOSO REIGADA, A., *Transparencia administrativa y protección de datos personales…*, *op.cit.*, pp. 43 y ss.

física identificable, no hay dato personal, en cuyo caso ni siquiera se plantea la aplicación del art. 18.4, debiendo accederse a lo solicitado sin más argumentos[763].

Estamos ante el enfrentamiento de dos derechos, la protección de datos personales y el acceso a la información pública sanitaria o de salud, que no son contrapuestos; pudiendo compatibilizarse, aunque puedan entrar en conflicto. Por ello, dado que las normas en conflicto tienen fundamentos distintos: las propias sobre protección de datos, la confidencialidad; y la de transparencia, la accesibilidad, resulta necesario, como decíamos, conciliar ambas en una aplicación equilibrada.

Señala FERNÁNDEZ RAMOS[764] que, en este particular enfrentamiento de derechos, se ha producido una colisión de leyes, cuando una ley ordinaria -la LTBG- entra a regular una materia (protección de datos, art. 15) que es objeto específico de una ley orgánica -LOPD- y, sin embargo, resulta necesaria determinar la normativa aplicable cuando la información contiene datos personales; de forma que, se aplicaría la LTBG si dicha información contiene datos personales de terceros, y si contiene datos personales del propio solicitante se aplicaría la normativa sobre protección de datos; por cuanto el derecho de acceso forma parte esencial del contenido fundamental a la protección de datos[765], y el régimen previsto en el art. 15 LOPD permanece vigente, al tratarse de un régimen especial que es excepcionado por la propia disposición adicional primera de la LTBG.

[763] CTPD Andalucía, RES/042/2016, de 22 de junio de 2016.

[764] FERNANDEZ RAMOS, S., *Acceso a la información pública versus protección de datos personales*, *op.cit*., p.6

[765] STC 292/2000, que señala que resulta indiscutible que el derecho de acceso que se encuentra recogido en el art. 8.b) y c) del Convenio 108 del Consejo de Europa y 12 y 13 de la Directiva 95/46 CE (derogada), forma parte del núcleo esencial del derecho regulado en el art. 18.4 CE.

2. LA NORMATIVA SOBRE PROTECCIÓN DE DATOS COMO LÍMITE AL ACCESO A LA INFORMACIÓN PÚBLICA SANITARIA

2.1. LA PROTECCIÓN DE DATOS COMO LÍMITE. EN ESPECIAL LOS DATOS DE SALUD

Tras la publicación del RGPD y de la LOPDGDD se plantean, como hemos visto, las relaciones entre la normativa sobre protección de datos y el derecho de acceso a la información pública regulado en la LTBG, en el sentido de determinar la prevalencia de uno de los dos derechos en el caso de una colisión entre ambos, como consecuencia de una solicitud de acceso a información pública cuyo contenido incluye datos personales de un tercero, que deben ser objeto de protección.

Por parte del RGPD, se refiere a la posibilidad de acceso a la información (documentos oficiales) en poder de las autoridades públicas (incluso de una entidad privada), para la realización de una misión de interés público, previendo que puedan existir colisiones con la protección de los datos personales; que habrán de resolverse conciliando los intereses en juego en la forma que se establezca por el Derecho de los Estados miembros[766].

Siguiendo con el análisis del art. 86 RGPD, la indicada necesidad de conciliación del derecho a la información con el derecho a la protección de datos personales no puede interpretarse de forma que deje sin contenido aplicativo este precepto, sino que deberá acudirse a la regulación específica para el derecho de acceso dictada por cada Estado miembro.

Como hemos visto anteriormente, el art. 9.2 RGPD, se refiere a los supuestos de habilitación del tratamiento de salud, al margen del consentimiento del interesado, levantando la prohibición del art. 9.1. Así, el apartado 2.b) del art. 9 RGPD, es susceptible de aplicación en el ámbito de la seguridad social y de los servicios sociales, conectados

[766] Art. 86 RGPD:
"Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento".

con la asistencia socio-sanitaria; el apartado 2.c), aplicable al ámbito de la salud, por su conexión con el derecho preferente a la vida; el apartado 2.e), en cuanto se trate de datos sanitarios que el interesado haya hecho públicos previamente; el apartado 2.g), relativo a datos de salud con un contenido no sanitario, como los seguros de salud, necesitándose de una ley habilitante.

Los últimos apartados del art. 9.2, h), i) y j), afectan al tratamiento de categorías especiales de datos personales relacionados con el ámbito sanitario; es decir, la asistencia sanitaria, la salud pública y la investigación en salud y biomédica; cuya habilitación para el tratamiento de este tipo de datos está basada en una norma con rango de ley, que debe adecuarse al principio de proporcionalidad.

Sin embargo, una norma con rango de ley que reconozca el derecho de acceso a la información pública podrá limitar los derechos sobre protección de datos de una persona, por cuanto el RGPD en su art. 23, autoriza a que mediante medidas legislativas del Derecho de la Unión o de los Estados miembros puedan limitarse el alcance de estos derechos, en la medida en que " (…) *tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar"; en concreto, la protección del interesado o de los derechos y libertades de otros*" (apartado i).

2.2. TIPOLOGÍA DE DATOS PERSONALES REGULADOS EN LA LTBG Y SU APLICACIÓN

Puede apreciarse como, en la normativa sobre protección datos personales, a diferencia de la LTBG, no hay conexión alguna con la normativa de acceso a la información, aunque permite que puedan proporcionarse en el ejercicio de las competencias legales o de lo dispuesto en la ley; de forma que, tratándose de una norma especial, se aplicará con carácter general la LTBG a la publicidad activa y a las solicitudes de información. Sin embargo, el derecho de acceso de una persona a sus propios datos personales se regirá por la normativa sobre protección de datos (art. 13 LOPDGDD) (derecho de acceso a la HC, por ejemplo), pero por esta vía no podrá solicitarse el acceso al resto de la información, si la hubiera, ya que estaríamos ante una vía diferente de acceso: precisamente la regulada en la LTBG.

Siguiendo a GUICHOT, podemos clasificar los distintos tipos de datos personales contenidos en el art. 15 LTBG mediante la existencia de tres círculos de protección[767]:

a) El círculo interno, que coincide con el de los datos especialmente protegidos, que no pueden ser facilitados a un tercero sin el consentimiento del afectado; o que lo establezca una ley, o que los haya hecho públicos el propio titular.

b) El círculo externo, constituido por los datos meramente identificativos relacionados con la organización, funcionamiento o actividad del órgano (art. 15.2), en los que, "con carácter general, prevalece la transparencia, salvo que, en el caso concreto, prevalezca la protección de datos u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida".

c) El círculo intermedio tiene carácter residual respecto de los datos no incluidos en las dos categorías anteriores; siendo necesario ponderar motivadamente por los Consejos de Transparencia el interés público en divulgar la información y los derechos de los afectados en cuanto a los datos que figuren en dicha información, y en especial los datos de carácter personal.

El art. 15 LTBG constituye "la clave de bóveda de todo el edificio en el que se concilian ambos derechos, y la conciliación se alcanza de una forma lógica, razonada y proporcionada"[768]. Así, es el precepto que regula específicamente la relación entre el derecho de acceso a la información pública y la protección de datos de carácter personal, ofreciendo soluciones diferentes por cada categoría de datos, en forma de exenciones o limitaciones para cada una de estas categorías; aunque en unas, particularmente, señala sí sería posible o no el acceso a la información; y, en otras, indica cuando es requerido el consentimiento específico, informado e inequívoco del afectado[769].

De esta forma, la LTBG "establece un régimen más o menos estricto de acceso a la información en función del mayor o menor nivel de protección de que disfruta el dato

[767] GUICHOT REINA, E., "Transparencia y protección de datos en las Universidades públicas", *Revista española de Derecho Administrativo* num.*193/2018*, parte Estudios, Editorial Civitas, Pamplona. 2018, pp.5-6.
[768] ENÉRIZ OLAECHEA, *op.cit.*, pp. 66 y ss.
[769] *Ibid.*, pp. 7-12.

específico cuya divulgación se pretende"[770]. Así, el máximo nivel de tutela se proporciona a los datos especialmente protegidos, conforme a la regulación del art. 9 RGPD, sin que, por parte de la LOPDGDD, se establezca una regulación concreta sobre el tratamiento de este tipo de datos, estableciendo, para los datos de salud (entre otros de su categoría especial), que "(…) *el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley* (art. 15.1 LTBG.

Además, estas reglas para solucionar los supuestos de acceso que surjan podrán ser completadas mediante los criterios de aplicación dictados por la AEPD y el/los Consejo/s de Transparencia, *"(...) en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma*", añadiendo "(…) *de conformidad con lo dispuesto en esta Ley y en la Ley Orgánica 15/1999, de 13 de diciembre* "(Disp.Adic.5ª); lo que parece superfluo, dada la aplicación preferente de la norma especial como es la LTBG.

Así, las reglas del artículo 15[771] de la LTBG han resultado suficientes para resolver cualquier supuesto donde se manifieste el conflicto de los derechos en cuestión, pero, la misma ley, en su poco clara Disp.Adic.5ª, sugiere a la CTBG y a la AEPD aplicar los criterios de aplicación previstos en ella, así como lo que estaba dispuesto en la LOPD; que, como señalábamos, pese a no estar vigente, en este caso puede cumplir una función interpretativa importante.

No obstante, pese a esta constante llamada a la ponderación suficientemente razonada de los distintos derechos e intereses en liza, actuantes en cada situación, cabe la posibilidad -como parece estar sucediendo- que después de ya los numerosos fallos del Consejo de Transparencia, tanto nacional como autonómicos, esta materia se aplique de forma uniforme y estandarizada, no solamente por la propia dinámica de las resoluciones administrativas de los casos planteados, sino por la propia LTBG, que en su art. 38.2.a) permite que se "(…) *adopten criterios de interpretación uniforme de las obligaciones*

[770] CTPD Andalucía RES/042/2016, de 22 de junio de 2016.

[771] No se aplica el artículo 15 de la LTBG si el acceso se efectúa previo procedimiento de disociación de los datos personales, de modo que se impida identificar a los titulares de la información.

contenidas en esta ley (…)"[772]; lo que implica, a juicio de C[773], que el CTBG disponga de competencias que deberían apoyarse en la propia norma; la cual, sin embargo, no determina como deben interpretarse.

Como veremos seguidamente en el procedimiento interno que debe realizar el sujeto público al que se solicita la información, después de examinar las causas de inadmisión se pasa al examen de aplicación de los límites, y, si se observa que existen datos personales, entra a su valoración conforme al art. 15 LTBG, que clasifica los tipos de datos personales de personas físicas, de acuerdo a la protección legal y facilidad de acceso (de menor a mayor grado), que se le brinda al ciudadano que solicita la información.

2.2.1. CATEGORÍAS ESPECIALES DE DATOS: DATOS DE CONTENIDO SANITARIO

De acuerdo con la clasificación de los datos personales prevista en el art. 15 LTBG, el primer nivel de protección lo ocupan los datos especialmente protegidos. Así, tratándose de datos de especial protección se excluyen los otros dos métodos de ponderación obligatorios que afectan a otros límites: el test de daño que se presume en todo caso y la técnica de la ponderación de intereses.

El art. 15 de la LTBG contempla dos tipos de datos personales especialmente protegidos; mientras la normativa de protección de datos acoge tres modalidades, en sus artículos 8 a 10 de la LOPDGDD: "Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos, tratamiento de datos de naturaleza penal y, lo que denomina "categorías especiales de datos", que incluye la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico; para los que el RGPD, en su art. 9, señala como "(…) 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

[772] Así como en su desarrollo, según el art. 8.2.b) RD 919/2014, de 31 de octubre, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno.
[773] JUNCEDA MORENO, J., "Obligaciones sobre transparencia. Protección de datos. Sobre los límites de la transparencia en el ámbito local", *La Administración Práctica*, nº 8/2016, Aranzadi, 2016.

persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física*(…)*", cuyo tratamiento queda prohibido.

Por tanto, el RGPD, respecto del contenido de datos especialmente protegidos que preveía la LOPD (art. 7) lo ha aumentado, incluyendo los datos genéticos, biométricos y

De ello resulta que, el régimen de acceso a información pública, cuando esta contenga datos de especial protección, previsto en el art. 15, contempla dos tipos de datos: los regulados en los arts. 7.2 y 7.3 de la LOPD, a los que, como señalábamos, deberán añadirse los datos especiales incorporados por el RGPD.

Tratándose de datos previstos en el art. 7.2 LOPD[774], únicamente podrá concederse el acceso solicitado con el consentimiento expreso y escrito del afectado, a solicitud del sujeto público actuante; se excepciona la prestación del consentimiento del afectado en el caso de que éste, con anterioridad a la solicitud de acceso, hubiese hecho públicos los datos de que se trate (art. 15.1 LTGB), en línea con lo señalado con el art. 9.2.e) del RGPD, que, igualmente, excepciona la necesidad de consentimiento cuando "(…) *el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos*".

En cuanto a los datos que hagan referencia al origen racial, a la salud y a la vida sexual (art. 7.3. LOPD) y los relativos a la comisión de infracciones penales o administrativas que no conlleven la amonestación pública del infractor (art. 15.1 LTBG)[775], sólo podrá concederse el acceso si se cuenta con el consentimiento expreso del afectado o si aquel

[774] "Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan 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 afectado".

[775] Por tanto, no será necesario el consentimiento expreso del afectado cuando se trata de sanciones que si conllevan amonestación pública del infractor, precisamente por el carácter público de las mismas derivado de su publicación en el diario oficial. Así, el art. 26.1 de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio de alto cargo de la Administración General del Estado, o en las normas autonómicas, como el art. 16.1 de la Ley 3/2005, de 8 de abril, de incompatibilidades de Altos Cargos de la Administración de la Junta de Andalucía y de Declaración de Actividades, Bienes e Intereses de Altos Cargos y otros Cargos Públicos.

Se excluyen del acceso la información relativa a los procedimientos administrativos sancionadores (incluidos los disciplinarios), en tramitación o ya finalizados.

estuviese amparado en una norma con rango de Ley[776]. A diferencia del apartado anterior, no se exige que el consentimiento sea por escrito, lo que nos trae a colación lo señalado en el título anterior respecto de la necesidad de constancia de que se ha prestado el consentimiento, así como la especial configuración de la prestación del consentimiento en el ámbito de la asistencia sanitaria, en el que, por sus propias especificidades, la regla general es la exigencia del consentimiento verbal.

Del mismo modo, la propia LTBG, exceptúa la necesidad de consentimiento del afectado en aquellos casos en que el acceso "estuviera amparado en una norma con rango de Ley" (art. 15.1)[777].

Esta excepción, como hemos visto, tiene gran trascendencia en el ámbito de la asistencia sanitaria[778], en concreto respecto del acceso a la Historia clínica: tanto por los profesionales sanitarios que atienden al paciente, en cuyo caso la LBAP exige que dicha excepción se interprete restrictivamente; de forma que el acceso habrá de ser concreto y

[776] Art. 7.3. LOPD. Para la redacción de este artículo el legislador tuvo en cuenta el criterio de la AEPD, por el que corresponde al legislador establecer la normativa especial que permita supuestos de acceso, debido a que los datos sobre la comisión de infracciones contienen una valoración negativa de una persona.

[777] Art. 15.1. LTBG:

"1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley".

[778] Con relación al tratamiento de datos relacionados con la salud y datos genéticos, se encuentran amparados en las letras g), h), i) y j) del art. 9.2 RGP, regulados en las siguientes leyes y sus disposiciones de desarrollo:

"1.

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

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.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

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.

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." (Disp.Adic.17ª LOPDGDD)".

proporcional o estrictamente necesario para cumplir con la finalidad para la que se accede, sin que pueda utilizarse para finalidades distintas.

Respecto del acceso de terceros, la LBAP, en su art. 16, se refiere al acceso a la HC con fines judiciales, epidemiológicos, de salud pública y de investigación o de docencia, en los que, para preservar el anonimato del paciente, será necesario separar los datos identificativos del paciente de los puramente clínicos o asistenciales, salvo que la autoridad judicial considere imprescindibles la unidad de los datos clínicos y los identificativos.

Además, los datos relacionados con la investigación en salud y biomédica, deberán ser objeto de seudonimización con carácter general, requiriéndose necesariamente el consentimiento, salvo situaciones de especial relevancia y gravedad para la salud pública (Disp.Adic.17ª.2 LOPDGDD).

A falta de habilitación legal, la manifestación formal del consentimiento por el tercero afectado e identificado se llevará a cabo procedimentalmente en el trámite de audiencia. Así, en el supuesto de que la información solicitada pudiera afectar a derechos o intereses de terceros, debidamente identificados, se les concederá un plazo de quince días para que puedan realizar las alegaciones que estimen oportunas, debiendo pronunciarse sobre si otorga o no el consentimiento; de forma que su oposición no impide que el órgano administrativo conceda el acceso total o parcial sin disociación, motivando y sopesando las razones que lo justifican[779]. El solicitante deberá ser informado de la suspensión del plazo para dictar resolución hasta que se hayan recibido las alegaciones o haya transcurrido el plazo para su presentación (art. 19.3 LTBG).

En el caso de datos relativos a la comisión de infracciones administrativas, que no comporten amonestación, el art. 15.1 LTBG, permite el acceso "(…) *en caso de que se cuente con el consentimiento expreso del afectado o si el acceso estuviera amparado en una norma con rango de Ley*"; lo que se traduce en la imposibilidad de concesión del acceso a los procedimientos administrativos sancionadores.

[779] No olvidemos que igualmente el sujeto público puede comunicar el acceso en el caso de que el afectado hubiera hecho públicos alguno de los distintos tipos de datos incluidos en la categoría de datos especialmente protegidos.

Como señalábamos al principio de este apartado, tratándose de datos especialmente protegidos no resulta necesaria la ponderación de intereses aplicable a los demás tipos de datos personales, por cuanto el consentimiento prestado elimina la necesidad de ponderación; y si no se hubiera prestado el consentimiento, tampoco sería necesaria la ponderación, ya que no puede accederse a la solicitud sin consentimiento, y la ponderación no puede suplirlo. Sin embargo, tratándose de datos manifiestamente públicos (art. 15.1), la innecesaria prestación del consentimiento del afectado obliga a ponderar previamente los perjuicios e intereses en juego[780].

En el caso de una solicitud de acceso al Gobierno del Principado de Asturias de un informe emitido por el Servicio de Prevención de riesgos laborales, el CTBG tras considerar que el contenido del informe contiene referencias a la salud de un tercero y, por tanto, tratarse de datos especialmente protegidos, deniega el acceso al no existir consentimiento del titular afectado ni de que exista una ley habilitante que disponga expresamente la cesión de datos a un tercero[781].

[780] PIÑAR MAÑAS, J.L. *Transparencia, acceso a la información y protección de datos*, *op.cit*., pp. 55-60.

[781] CTBG, R. nº 284-RT/2016, de 16 de marzo de 2017.

2.2.2. ACCESO A INFORMACIÓN QUE NO CONTIENE DATOS ESPECIALMENTE PROTEGIDOS

No obstante ser el objeto de este trabajo el estudio de la protección de datos en el ámbito de la salud y, en concreto de este capítulo III, su examen junto con el derecho de acceso a la información pública sanitaria, considero que puede ser útil disponer de una visión de conjunto del contenido y sus condiciones de tratamiento, en relación con la tipología de datos personales contenida en la LTBG. A continuación, se incluye un cuadro sinóptico al respecto.

Tabla 1. *Datos personales meramente identificados relacionados con la organización, funcionamiento o actividad pública de un órgano administrativo*

Contenido	Solicitante	Ventaja	Condición para su tratamiento
Nombre y apellido Cargo, puesto o función Titulación profesional o universitaria Direcciones postales, electrónicas, números de teléfono y fax del lugar de trabajo	Cualquier Ciudadano	Se pueden tratar y comunicar a terceros No se puede negar invocando protección No se requiere consentimiento ni audienc	No es aplicable a datos referidos a personas jurídicas. Se trata de información de la persona en el ejercicio de funciones propias de las Administraciones públicas y en el ámbito de las competencias. La comunicación será legítima si se limita a la finalidad que la justifique.

Tabla 2. *Datos personales meramente identificativos*

Contenido	Solicitante	Ventaja	Condición para su tratamiento
Nombre y apellido de persona mayor de edad Datos que no guarden relación con la organización, funcionamiento o actividad pública del órgano administrativo. Información como direcciones postales, electrónicas o números de teléfono sólo si ha sido autorizada su inclusión en fuente accesible al público por el afectado.	Si reúne la condición de «interesado» en un procedimiento administrativo o Es titular de un derecho o interés legítimo que puede haberse visto afectado por la actuación de la persona física cuyos datos identificativos se solicitan.	Pueden ser comunicados a un tercero sin consentimiento del afectado. Cuando se produzca con el objeto de ejercer un derecho en juicio.	El órgano administrativo debe ponderar los derechos e intereses en juego. Debe razonar de manera suficiente, tanto la ponderación como la decisión que adopte en una resolución administrativa.

Tabla 3. *Datos personales "ordinarios" o no especialmente protegidos*

Contenido	Solicitante	Ventaja	Condición para su tratamiento
Nombre y apellido de persona mayor de edad Datos que no guarden relación con la organización, funcionamiento o actividad pública del administrativo. Información como direcciones postales, electrónicas o números de teléfono sólo si ha sido autorizada su inclusión en fuente accesible al público p afectado.	Si reúne la condición de «interesado» en un procedimiento administrativo c Es titular de un derecho o interés legítimo que puede haberse visto afectado por la actuación de la persona física cuyos datos identificativos se solicitan .Tenga la condición de investigador y haya motivado el acceso en un carácter histórico, científico o estadístico.	La oposición del tercero a facilitar la información no impide por sí sola la comunicación, sino que obliga al órgano competente a ponderar tal oposición y, en caso de considerar que debe prevalecer el derecho de acceso, sigue motivar su resolución. No puede considerarse oposición la de personas jurídicas que aparezcan procedimiento en defensa de la persona física titular del dato personal. Es accesible cuando se aprecie un mayor peso del interés público en divulgar la información que en la protección de los datos personales que aparecen en la información solicitada.	El órgano administrativo debe ponderar los derechos e intereses en juego: el interés púb la divulgación de los datos identificativos derechos de los afectados y, en particular, su derecho fundamental a la protección de datos de carácter personal. Debe razonar de manera suficiente, tanto la ponderación como la decisión que adopte en una resolución administrativa. El órgano competente debe conceder un plazo de quince días al titular del dato (que es una persona física debidamente identificada) para que pueda presentar las alegaciones que estime oportuno. Concluido el trámite de alegaciones, y con todos los elementos encima de la mesa, el órgano debe decidir acerca de si facilita el acceso solicitado o no. Hayan transcurrido los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del patrimonio histórico español.

Tabla 4.*Datos personales especialmente protegidos*

Contenido	Solicitante	Ventaja	Condición para su tratamiento
Datos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos genéticos, los datos biométricos que permitan identificar a una persona física , los datos relativos a la salud, y los datos relativos a la vida sexual o a la orientación sexual persona física. Datos personales relativos a condenas e infracciones penales y a las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad información.	Si reúne la condición de «interesado » en un procedimiento administrativ Es titular de un derecho o interés legítimo que puede haberse visto afectado por la actuación de la persona física cuyos datos identificativos se solicitan.	No se requiere consentimiento del afectado cuando esta persona hubiese manifiestamente públicos los datos con anterioridad a que se solicite el acceso, lo cual deberá quedar acreditado en la resolución que autorice el acceso. Tampoco es preciso obtener el consentimiento si el acceso estuviera amparado por una norma con rango de Ley. La legislación sanitaria puede permitir el acceso a información pública de terceros en determinados supuestos y con determinadas garantías.	Si la información se trata de datos sobre la ideología, religión, creencias y afiliación sindical, el órgano competente solo puede autorizar el acceso cuando se cuente con el consentimiento expreso y por escrito del afectado., que deberá recabar dicho órgano (no podrá trasladar esta carga al solicitante de la información). Cuando la información contiene datos que hacen referencia al origen racial o étnico, a datos genéticos o biométricos, a la salud, a la vida sexual u orientación sexual y a comisión de infracciones penales o administrativas que no conlleven amonestación pública al infractor, el órgano competente solo puede autorizar el acceso en caso de que cuente con el consentimiento explícito del afectado (basta dejar constancia en el expediente). Si la información solicitada puede afectar a derechos o intereses de terceros, debidamente identificados el órgano competente debe concederles un plazo de quince días hábiles para que puedan realizar las alegaciones que estimen oportunas y, en consecuencia, manifestar que otorgan su consentimiento o, por el contrario, se oponen a concederlo.

3. PROCESO APLICATIVO PARA RESOLVER LA SOLICITUD DE ACCESO A LA INFORMACION EN EL ÁMBITO SANITARIO

3.1. VALORACION ACERCA DE SI LA INFORMACION SOLICITADA CONTIENE DATOS PERSONALES

El Real Decreto 463/2020 de 14 de marzo, que determinó el estado de alarma, además de otras medidas, dispuso la suspensión de los procedimientos administrativos, incluyendo la paralización, desde el 14 de marzo de 2020, de las solicitudes de acceso a información pública previstas en la LTBG, así como las reclamaciones ante el CTBG; coincidente con una gran demanda de solicitudes tanto por ciudadanos como por la prensa periodística.

La Dirección General de Gobernanza Pública (Ministerio de Política Territorial y Función Pública), como gestora del Portal de Transparencia, trasladó a las distintas unidades de transparencia que, como criterio general, no notificaran las resoluciones, aunque sí deberían seguir tramitándose; al mismo tiempo, que recordaba que las excepciones para no aplicar la suspensión debían aplicarse decidiendo caso por caso y de forma motivada.

En relación con la indicada suspensión, la Abogacía del Estado dictaminó que debe suspenderse tanto el trámite de petición como el de reclamación ante el CTBG, pudiendo reanudarse (7 de mayo de 2020) una vez finalice el estado de alarma. Por tanto (durante el estado de alarma) no puede realizarse notificaciones de una resolución dictada ni que el CTBG solicite el trámite de alegaciones a las unidades de transparencia en un procedimiento contra una denegación de acceso, ni tampoco se pueden resolver reclamaciones contra una denegación de acceso.

Del mismo modo, la Abogacía del Estado considera que "la suspensión de los procedimientos referidos no vulnera el derecho de acceso a la información pública, pues lo que hace la medida -excepcional y transitoria, adoptada por razones de política sanitaria, para coadyuvar a la consecución de las medidas para combatir la crisis sanitaria- es demorar la tramitación del procedimiento, suspendiéndolo y previendo expresamente su reanudación una vez desaparezca el estado de alarma, de modo que ningún derecho subjetivo ni interés legítimo resulta lesionado por la mera suspensión".

No obstante, señala que existen excepciones, contenidas en el propio Real Decreto relativas a la suspensión de procedimientos administrativos, como la de "considerar que

viene referido a situaciones estrechamente vinculadas a los hechos justificativos del estado de alarma, o que es indispensable para la protección del interés general o para el funcionamiento básico de los servicios". De esta forma, las administraciones públicas podían atender los procedimientos directamente vinculados con el estado de alarma, y, por tanto, para las solicitudes de información sobre la COVID-19.

Como tal excepción, hay que considerar la solicitud planteada por una sociedad periodística ante el Instituto de Salud Carlos III (que aglutina todos los datos del Estado sobre la pandemia), sobre todos los casos de coronavirus producidos, como la edad de cada enfermo o los síntomas que padece y la fecha desde que comenzó a tenerlo; a fin de conocer más información sobre la incidencia del coronavirus en nuestro país. La situación ha sido denegada en base a la necesidad de reelaborar la información y la imposibilidad de revelar datos personales (de salud). No obstante, podría haberse accedido a conceder un acceso anonimizado de datos.

Debemos tener en cuenta, a la hora de permitir o denegar el acceso a la información pública, la STJUE de 24 de noviembre de 2011, por la que se señala que es contrario a Derecho comunitario la exigencia del art. 6.2 de la LOPD (aplicable en el momento de la sentencia), de que los datos figuren en fuentes accesibles al público para permitir el acceso de un tercero con un interés legítimo (concepto al que nos hemos referido en el apartado 2.1 al tratar el consentimiento). El sentido de esta sentencia ha sido asumido por distintas sentencias nacionales, en especial la SAN de 26 de noviembre de 2013, que indica, tomando como base la STJUE, que:

> *"(…) los datos que figuren en fuentes accesibles al público no es un criterio válido para excluir la necesidad de consentimiento del titular de los datos -ni para exigirlo forzosamente- sino que en aplicación del art. 7.f.) de la Directiva 95/46/CE, deben ponderarse dos elementos fundamentales:*
>
> *-Si el tratamiento de los datos es necesario para satisfacer un interés legítimo (del responsable de los datos o del concesionario);*
> *-Y si han de prevalecer o no los derechos fundamentales del interesado, esencialmente referidos a su derecho a la protección de datos personales.*
>
> *Ponderación de intereses en conflicto que dependerá de las circunstancias concretas de cada caso y en la que, no obstante, si puede tomarse en*

> *consideración, a efectos de determinar la posible lesión de los derechos fundamentales del afectado, el hecho de que los datos figuren ya, o no, en fuentes accesibles al público. Más ello, simplemente, como un elemento más de ponderación".*

Por tanto, en el ámbito del proceso interno de resolución de la solicitud de información pública a realizar por el órgano administrativo, una vez determinado que no resulta procedente la inadmisión de la solicitud, debe procederse a entrar a valorar si la información solicitada contiene o no datos personales. La mayoría de las CCAA y el Ministerio de Sanidad han incorporado en sus páginas web espacios concretos para informar sobre el acceso a datos de salud de acuerdo con la Ley de Transparencia, bien de su Comunidad o la estatal[782].

Así, en el caso de acceso a un expediente que contenga datos personales deben ponderarse los derechos del solicitante, así como del titular de los datos; de forma que el hecho de que estos datos figuren en una fuente de público acceso sólo será un criterio más a favor de la consideración del acceso del solicitante al expediente.

En el supuesto de que la información solicitada contuviera al mismo tiempo datos personales del solicitante y datos de terceros procedería aplicar la LTBG, por cuanto el derecho de acceso no alcanza a los datos personales de un tercero[783]. "Esta ponderación es al mismo tiempo la clave bóveda y el Caballo de Troya de la relación y convivencia entre el acceso a la información y la protección de datos"[784].

Además, las resoluciones que se dicten "(…) *serán objeto de publicidad previa disociación de los datos de carácter personal que contuvieran y sin perjuicio de lo dispuesto en el apartado 3 del artículo 20, una vez hayan sido notificadas a los interesados*" (art. 14.3).

[782] P.ej. para Castilla y León: https://www.tramitacastillayleon.jcyl.es/web/jcyl/AdministracionElectronica/es/Plantilla100Detalle/1251181050732/_/1284539839313/Tramite.

[783] SAN de 30 de junio de 2011, dictada en relación con la petición de un profesor de la ANECA de acceder no sólo a sus datos personales además de a la de los datos de todas las personas que accedieron al expediente de tramitación de la acreditación de que se trataba.

[784] PIÑAR MAÑAS, *Transparencia, acceso a la información y protección de datos*, *op.cit*., p .60.

3.2. ANÁLISIS ACERCA DE SI LA INFORMACIÓN CONTIENE DATOS DE SALUD

La indiscutible trascendencia del derecho a la protección de la salud se manifiesta a través de las distintas normativas (estatales y autonómicas) que regulan toda la estructura organizativa (medios personales y materiales) y de prestación del SNS, y que permiten y tutelan el derecho a la salud. Para el funcionamiento y mantenimiento de este modelo (de acceso universal, gratuito y descentralizado) es necesario una cantidad ingente de actuaciones tanto de contenido propiamente asistencial, sanitario o de salud, como de otro tipo, planificaciones, estadísticas, informes, estudios, etc., que agrupadas bajo el concepto de "información pública" pueden ser objeto de acceso por los ciudadanos.

A diferencia de lo que constituye el acceso a la historia clínica de un paciente, tanto por el propio paciente como por los profesionales sanitarios para su atención, y por terceros legalmente autorizados, como hemos visto en el título anterior, en este caso estamos ante un procedimiento distinto de acceso, ya que el contenido de la información a solicitar es distinta, no se trata de la HC de un paciente, sino de contenidos o documentos que obran en poder de las Administraciones públicas, elaboradas o adquiridas como resultado de sus funciones. Sin embargo, pese a la importancia de la información como instrumento de participación de los ciudadanos y el control democrático de los gobernantes, tiene sus límites, básicamente la protección de la intimidad privada.

Así, es posible que en el caso de una solicitud de acceso en la información ésta incluya en su contenido datos personales de salud (como, por ejemplo, de una subvención a pacientes de ELA), que en este caso se trataría de datos sensibles o especialmente protegidos, lo que cualifica doblemente la necesidad de protección de la intimidad personal de su titular, conforme se ha señalado al tratar la categoría de datos especialmente protegidos (apartado 3.2.1).

Por ello, estamos ante una interacción de dos derechos en la que es necesario buscar un equilibrio, de forma que exista una complementariedad entre ellos, a fin de que se permita a cualquier persona disponer de información de carácter sanitario; al mismo tiempo que el sujeto administrativo solicitante no puede suministrarla sin que el titular de los datos dé su consentimiento.

Resulta relevante señalar la sentencia del TEDH[785], dictada en sus inicios, pronunciándose sobre la revelación de datos de salud (sobre la condición de seropositiva de la solicitante) en un proceso penal seguido contra su esposo. El TEDH, tomando como base el art. 8 CEDH, reconoce la importancia de la protección del derecho a la privacidad, en especial cuando se refiere a datos de salud, señalando que la legislación de cada Estado debe adoptar las garantías necesarias para impedir la divulgación de datos personales de salud.

Otra sentencia especialmente notable dictada por el TEDH en sus inicios fue la del caso *Z v. Finlandia*, en donde se pronunció sobre la revelación de datos de salud – condición de seropositiva de la peticionaria– en un proceso penal que se seguía en contra de su esposo. El TEDH mencionó en forma expresa al artículo 8 del CEDH y también se refirió por primera vez a la aplicación del Convenio 108. El TEDH reconoció la trascendencia de la protección de datos de carácter personal para el ejercicio del derecho a la privacidad contenido en el artículo 8 del CEDH, en especial cuando a datos de salud se refiere y señala que la legislación interna debe adoptar las garantías necesarias para impedir la divulgación de datos personales relativos a la salud.

3.3. PONDERACIÓN PARTICULARIZADA DE INTERESES

3.3.1. CRITERIO DE LA PREVALENCIA DEL INTERÉS PÚBLICO

Podemos decir, que, a diferencia de los datos relativos a la protección de datos de carácter personal, que se aplican directamente, los límites previstos en el art. 14 LTBG no se aplican directamente, por cuanto el propio apartado 1 señala que "podrán" ser aplicados. De ahí, que no se aplican automáticamente a favor de la denegación ni de forma absoluta respecto de sus contenidos, sino para cada caso concreto.

Así, la apreciación de motivos de interés público a fin de limitar o denegar el acceso solicitado deberá estar asociada con la existencia de un interés racional y legítimo digno de protección; sin que, al mismo tiempo, tenga una aplicación automática, debiendo procederse a la ponderación de los intereses en juego: a evaluar previamente el perjuicio hipotético de carácter concreto y medible (test de daño), el cual no podrá afectar a un

[785] STEDH de 25 de febrero de 1997, caso Z. c. Finlandia (rec. núm. 9/1996), apartado 95.

determinado ámbito material (ya que ello excluiría a todo el bloque de información); y la existencia o no de un interés público que justifique la publicidad o el acceso (test del interés público); necesitando, así, una aplicación justificada y razonada aplicada para el caso concreto de que se trate[786].

La LTBG, se refiere a la especial consideración del interés público al señalar que: "*La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso*"[787]. Además, contiene un conjunto de excepciones que permiten la protección del interés público en materia de seguridad nacional, defensa o las relaciones exteriores; pero, no podemos inferir con ello que todo documento relacionado tenga la misma categoría o nivel si no se ha determinado previamente.

En relación con el interés público derivado de los documentos oficiales declarados secretos, sin dejar de reconocer que la normativa europea de seguridad (EEAS) prevé que un documento se mantenga de manera indefinida en su nivel de clasificación cuando se considere necesario[788], es lamentable que no se haya llevado a la práctica lo planteado en el art. 3 del Reglamento de la Ley de secretos oficiales, que señala "(…) *a efectos de evitar la acumulación excesiva de material calificado, la autoridad encargada de la calificación deberá señalar los procedimientos para determinar, periódicamente, la conveniencia de la reclasificación o desclasificación de aquel material"*[789].

De esta forma, la opacidad que podría estar presente en una solicitud de información, como advierten algunos autores, se extiende a casos como el derivado de la situación presentada por la aparición de los "*Wikileaks*"[790], en octubre de 2010, obligando al Consejo de Ministros español a adoptar el acuerdo de declarar secretos muchos de los

[786] CTBG, CI/002/2015, de 24 de junio de 2015.
[787] LTBG, Art. 14.2.
[788] PALACIOS, J. M., "Hacia la reforma de la Ley de Secretos Oficiales de 1968. Análisis GESI/Universidad de Granada". Disponible en: http://www.seguridadinternacional.es/?q=es/content/hacia-la-reforma-de-la-ley-de-secretos-oficiales-de-1968
[789] Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968 de 5 de abril sobre Secretos Oficiales.
[790] Se trata de una organización mediática internacional cuyos objetivos son sacar a la luz material sensible y clasificado de interés público. Su actividad se centró, inicialmente, en los años 2007 y 2008, sobre todo centrada en la política exterior norteamericana, especialmente con las guerras de Irak y de Afganistan.

escritos y notas diplomáticas, sin importar la fecha de su ejecución; incluyendo en su declaración de secreto al mismo acuerdo. De ello, se derivaba que el Ministerio de Exteriores negara el acceso a documentos con información acerca de las relaciones diplomáticas con Alemania o Filipinas entre 1970 y 1982, siendo la excusa que hayan sido clasificados por ese acuerdo desconocido de 2010. En 2013, un grupo considerable de historiadores españoles, apoyados por investigadores extranjeros, exigieron "la inmediata reapertura de los fondos históricos y la garantía de su accesibilidad para todos los investigadores en el plazo más breve posible".

En el caso de la solicitud de acceso a las retribuciones del personal directivo de RENFE, el CTBG, considera que no resulta posible apreciar que la información relativa a las retribuciones del personal directivo de una entidad pública pueda ser denegada invocando el límite de los datos de carácter personal, salvo que efectivamente haya afectación a su esfera personal, como puedan ser referencias a su domicilio personal o familiar, por cuanto en la medida que el acceso a la información "contribuya a un mejor conocimiento de los criterios de organización y funcionamiento de las instituciones o a la asignación de recursos, cabrá considerar la existencia de un interés público prevalente sobre los derechos a la protección de datos y a la intimidad en los términos y con las excepciones previstas en la LTBG"; primando el interés público sobre los derechos a la intimidad y a la protección de datos de carácter personal[791].

Igualmente, se aprecia la prevalencia del criterio del interés público en una solicitud de información sobre procesos electorales a un Colegio Profesional, en el cual el CTPD Andalucía, después de afirmar que la materia electoral "constituye uno de los ámbitos sobre los que puede proyectarse el ejercicio del derecho de acceso a la información pública", y considerar que supone estar incluidos en la vertiente pública si se trata de los aspectos organizativos de los Colegios profesionales[792], resuelve que "es manifiesto el interés público en que se difunda la información relativa al proceso electoral", procediendo que se faciliten las actas solicitadas[793].

Siguiendo con el trascendental criterio del "interés público", en el caso de una solicitud de conocer nombres y apellidos de empleados públicos del Ayuntamiento de Madrid, el

[791] CTBG, RE nº 406/2017, de 23 de noviembre de 2017.
[792] STC 20/1988, FJ 4.
[793] CTPD Andalucía, RES/85/2019, de 1 de abril de 2019.

CTBG, viene a considerar el Informe conjunto del Consejo y de la AEPD, de 23 de marzo de 2015, que señala que "en cuanto el acceso a la información contribuya a un mejor conocimiento de los criterios de organización y funcionamiento de las instituciones o a la asignación de recursos, cabrá considerar la existencia de un interés público prevalente sobre los derechos a la protección de datos y a la intimidad en los términos y con las excepciones establecidas por la LTBG. Por el contrario, cuando la información no contribuya a un mayor conocimiento de la organización y funcionamiento de las instituciones o de la asignación de recursos públicos, prevalecerá el respeto a los derechos a la protección de datos".

Lo que trasladado al caso en cuestión supone, que el criterio para delimitar el interés público prevalente de los puestos de la Administración se determine en base a aspectos como el mayor nivel de responsabilidad y la mayor autonomía de las decisiones, la existencia de discrecionalidad en el nombramiento o una confianza especial, casos estos en los que prevalece el interés público sobre la protección de datos, que, sin embargo, no ocurre con los restantes puestos de trabajo[794].

De esta forma, tratándose de solicitudes de información que no contengan datos especialmente protegidos relativas al personal público sujeto a la LTBG, se facilitarán únicamente los datos personales identificativos relacionados con la posición que ocupan en la organización del organismo público, considerando el mayor nivel de responsabilidad y la mayor autonomía de sus decisiones, la mayor discrecionalidad en su nombramiento, y una confianza especial, al existir en estos casos un interés prevalente sobre la protección de datos.

Sin embargo, ante una solicitud de copia del empadronamiento de varias personas al Ayuntamiento de Sevilla, el CTPD Andalucía, entiende que, al no haber datos especialmente protegidos, sino que son de carácter identificativo y muchos de ellos afectan a menores, no existe interés público en la divulgación, sino privado, de forma que éste no debe prevalecer sobre los derechos a la intimidad y a la protección de datos personales de los menores y sus familiares.[795]

[794] CTBG RE nº 132/2017, de 7 de agosto de 2017.
[795] CTPD Andalucía, RES/002/2017, de 4 de enero de 2017.

Se considera de interés público existente en la divulgación de una información que afecta a un servicio básico como es el de suministro de energía eléctrica, dada la innegable trascendencia social del suministro de este tipo de suministros, lo que justifica la apertura de la documentación solicitada[796].

En el caso de una solicitud de conocer "los gastos de alojamiento, manutención y de locomoción de los viajes institucionales (…) abonados a la Presidencia de la Junta de Andalucía y de las personas titulares de la consejería…", el CTPD Andalucía señala que resulta indudable que la información solicitada "tiene relevancia pública en la información de naturaleza económica, resultando por tanto del máximo interés para la divulgación de datos referentes a las decisiones de gasto por parte de las Administraciones Públicas: (…) resulta incuestionable que la información referente a la recaudación de recursos por parte de los poderes públicos y la subsiguiente utilización de los mismos constituye un eje central de la legislación en materia de transparencia" (por todas, Resolución 106/2016, de 16 de noviembre, FJ 4).

3.3.2. APLICACIÓN DE LA PONDERACIÓN DE LOS INTERESES EN JUEGO: EXCLUSIÓN DE LOS DATOS SANITARIOS

Puede decirse, sin duda alguna, que el aspecto y el efecto práctico más importante de la consideración jurídica de los datos especialmente protegidos en relación con la transparencia y el acceso a la información, resulta de la exclusión de la aplicación del régimen de ponderación y afectación al que si se encuentran sometidos los demás datos personales no especialmente protegidos[797]. Sin embargo, habrá que tener en cuenta el hecho de que el interesado los haya hecho públicos, en cuyo caso quedan sujetos a la ponderación que pueda realizar la Administración solicitante del acceso.

A ello, se refiere PIÑAR MAÑAS, señalando que en el caso de acceso a datos especialmente protegidos "siempre será necesario el consentimiento expreso del afectado, lo que hace

[796] CTPD Andalucía, RES/042/2016, de 22 de junio de 2016.

[797] RODRÍGUEZ ÁLVAREZ, J.L., "Transparencia y protección de datos personales: criterios legales de conciliación". En D. Canals Ametler (ed.), *Datos. Protección, Transparencia y Buena Regulación. 2016*, accesible en : www.documentauniversitaria.com.
Para más información sobre la ponderación de bienes e intereses, vide RODRÍGUEZ SANTIAGO, J.M., "La ponderación de bienes e intereses en el Derecho Administrativo", Marcial Pons, Madrid, 2000.

innecesaria la ponderación: si se cuenta con el consentimiento la cesión es posible sin que se requiera ejercicio de ponderación alguno, y si tal consentimiento no se da tampoco cabe ponderación porque ésta no puede habilitar una cesión que sólo es posible con el consentimiento del afectado. Esta regla tiene una excepción: los datos hechos manifiestamente públicos a que se refiere el artículo 15.1 párrafo primero, pues en este caso, al no ser necesario el consentimiento, será preciso llevar a cabo la ponderación con carácter previo a la comunicación de los datos"[798].

Por tanto, tratándose de datos de salud (y, por tanto, especialmente protegidos) sólo es posible acceder a la información solicitada contando con el consentimiento informado y expreso del titular afectado o existe ley habilitante, lo que, con GUICHOT REINA, nos permite señalar si estamos ante un régimen demasiado flexible para este tipo de datos, pudiendo preguntarse sobre si es necesario y pertinente haber adoptado un sistema que al menos hubiese permitido poder valorar si se concede el acceso a este tipo de datos, en aquellos casos de una manifiesta trascendencia pública de los mismos[799]. Sin embargo, no puede olvidarse la naturaleza y especial sensibilidad de los datos que se están manejando, de ahí, que hayan sido dotados de una especial rigidez, tanto por el art. 16.2 CE, como por la LOPDGDD y el RGPD; de forma que una ley ordinaria como la LTBG no puede limitarlos, como fue señalado por la AEPD en el informe sobre el Anteproyecto de la LTBG, refiriéndose a la LOPD.

[798] PIÑAR MAÑAS, J.L. (2014). *Transparencia y protección de datos… op. cit.* p. 60.

[799] En este sentido, GUICHOT REINA señala que "la opción del legislador, siendo armónica con la LOPD, es un tanto "positivista" y acaso podría pensarse que también en el caso de salud o de sanciones pudiera haber acogido un criterio último de ponderación con el interés público en la divulgación que permitiera excepcionalmente dar preferencia a este último en casos muy relevantes (el estado de salud de un alto cargo, incluyendo en particular los Presidentes de Gobiernos, relacionados con la capacidad para el ejercicio de sus funciones, las sanciones administrativas o disciplinarias impuestas a un alto cargo). Dicho de otra forma, si por ley singular se pueden establecer casos en que prevalece la publicidad de los datos sanitarios o sancionadores, tal vez en la ley general que regula la transparencia podría haberse acogido un principio más general de ponderación del interés público en la divulgación en casos relacionados con otros bienes constitucionales. (…) A mi juicio, lo más cuestionable es el efecto que supone respecto a la inaccesibilidad a la información sobre sanciones administrativas (salvo previsión legal expresa o que se trate de sanciones que conlleven amonestación pública), información que no resulta evidente que pertenezca a la intimidad de las personas y cuyo conocimiento en ocasiones es crucial para controlar la efectiva aplicación por igual de la ley a todas las personas. Más aún considerando que incluyen, si se sigue la interpretación que se maneja en el campo de la protección de datos, las sanciones disciplinarias cuyo conocimiento puede ser de suma relevancia pública para juzgar la actuación administrativa".
Vide GUICHOT REINA, E., "Límites a la transparencia y el acceso a la información", en GUICHOT, E. (Coord.), *Transparencia, acceso a la información pública y Buen Gobierno*…, *op.cit.*, pp. 97-141.

Fuera del ámbito sanitario (y de los datos especialmente protegidos) habrá que acudir, como hemos visto, al criterio del interés público para delimitar si una información es de interés general de la comunidad y, por tanto, deba prevalecer sobre intereses individuales. Para ello, se aplica el test de daño, por el que, en la medida en que, de concederse el acceso solicitado, el daño causado al Estado sería de mayor consideración que el provocado al particular denegando el acceso; al mismo tiempo que se evalúe el perjuicio que pudiera causar al afectado la revelación de sus datos. De ahí, que el sujeto público solicitante del acceso debe ponderar adecuadamente los distintos intereses en conflicto, procediendo, incluso, permitir el acceso de aquella información no afectada por una protección de privacidad.

Así, tratándose de información no comprensiva de datos especialmente protegidos, el órgano administrativo deberá proceder a una ponderación singularizada y "suficientemente razonada" de los derechos e intereses intervinientes en ese caso determinado, evaluando el interés público en la divulgación de la información y la influencia de los derechos de los afectados; por tanto, habrá de considerarse las circunstancias concretas de cada caso.

Por ello, se parte del juicio de proporcionalidad[800] a realizar seguirá los razonamientos habituales, en especial del juicio de constitucionalidad, sometidos a la posibilidad de revisión judicial; de forma que habría que hacer una valoración hipotética del daño que provocaría la comunicación de la información, siendo necesario que el daño sea sustancial para que la comunicación pueda juzgarse desproporcionada, y sin que en ningún caso la concesión del acceso pueda tener como resultado una vulneración del derecho a la protección de datos del afectado; por lo que, si se considera que esta situación puede producirse, el órgano debe plantearse recurrir a conceder el acceso parcial[801].

[800] Como señala BARNÉS, refiriéndose a la diferencia entre ponderación de bienes e intereses y principio de proporcionalidad, señala que "la ponderación constituye un género más amplio, que comprende y admite juicios o perspectivas diferentes, mientras que la proporcionalidad en sentido propio no es más que una de sus modalidades posibles, tan sólo preocupada por la razonable relación de costes y beneficios. El juicio de proporcionalidad, pues, como especie o variante de la ponderación de bienes e intereses". BARNÉS, J., "El principio de proporcionalidad. Estudio preliminar", *Cuadernos de Derecho Público*, n º 5, 1998, pp.34-35.

[801] GUICHOT REINA, E., "Un paso decisivo en la clarificación de las relaciones entre derecho de acceso y derecho a la protección de datos: La Sentencia del TPI de 8 de noviembre de 2007, Bavarian Lage/Comisión, T.194/04", *Revista Española de Derecho europeo*, nº 27/2008, Civitas, 2008, pp.18-19:
"El paso final es el test de proporcionalidad , que implica un acercamiento necesariamente casuístico, en que hay que analizar qué tipo de daño provocaría (o ha provocado, si se actúa ex post facto) la práctica la revelación, daño que debe ser sustancial para que la revelación pueda considerarse desproporcionada, sin

En este sentido, como señala la AEPD, "(…) la finalidad de otorgar información ambiental debe ponerse en consonancia con el principio de proporcionalidad y finalidad de los datos, que son piedra angular de la protección de datos, (…) pudiéndose comunicar la información siempre y cuando ésta no permita la identificación de personas físicas (…)"[802]. De forma que, resulta necesario examinar para cada caso concreto: si el fin a alcanzar es proporcional con el medio empleado, si resulta necesaria la intromisión en la intimidad personal, y las consecuencias negativas que puedan derivarse para el solicitante.

Sin embargo (art. 15.4 LTBG), no se aplicará lo dispuesto en los artículos anteriores si el acceso se efectúa previa disociación[803] de los datos de carácter personal de modo que impida la identificación de las personas afectadas. En este sentido, señalar, como, tanto la anterior LOPD, art. 11.6, no exigía consentimiento del interesado tratándose de datos anonimizados, y el RGPD, que excluía de su aplicación a la información anonimizada[804].

El Proyecto inicial de la LTBG venía a delimitar los campos de aplicación de la entonces LOPD y de la propia ley. Así, tratándose de información pública que contenga datos personales se aplicaría la LTBG; en cambio, si dicha información incluye sólo datos del solicitante, entonces se aplica la LOPD. Sin embargo, a la vista del informe del Consejo de Estado se suprimió este apartado del Proyecto de Ley. No obstante, algunas CCAA han regulado transparencia basándose precisamente en este apartado del Proyecto de Ley, de manera que únicamente se aplicaría la normativa sobre protección de datos cuando la información se refiere únicamente a datos personales del solicitante[805].

---

que en ningún caso la revelación pueda tener como resultado que una persona se vea privada o indebidamente restringida en su derecho fundamental a la protección de datos. Si (y sólo sí) se considera que se produciría esta situación, hay que plantearse si el acceso parcial (borrando únicamente los elementos del texto que causan un daño sustancial) o la anonimización sería una solución, ya que se trata de una excepción a la regla general de la plenitud del derecho de acceso. Puede ser por tanto una solución práctica si el daño a la intimidad del sujeto es sustancial y si el sujeto en cuestión no es la fuente primaria de interés para el público".

[802] AEPD, informe 0194/2010.

[803] Prevista en el art. 4.5. RGPD.

[804] RGPD, Considerando 26:

"Por lo tanto los principios de protección de datos no deben aplicarse a la información 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".

[805] Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno de Cataluña, art. 24.3, y Ley 2/2016, de 7 de abril, de Instituciones Locales de Euskadi, art. 62.4.

Partiendo del art. 11 LOPD, que, en su apartado a), en la comunicación de datos, exime de la necesidad de consentimiento cuando la cesión está autorizada por una ley, lo que hace la LTBG es establecer las condiciones específicas legitimadoras de la cesión de datos personales en el acceso a la información pública sin el consentimiento del interesado.

En este sentido PIÑAR MAÑAS[806], señala que para poder llevar a cabo la cesión de sus datos personales a terceros (los solicitantes de acceso) sin necesidad de consentimiento de los afectados sería necesaria una ley habilitante, y esta ley es la LTBG; lo que supone un giro total respecto a la legislación anterior, en la que la regla general era la necesidad de consentimiento para proceder al acceso de información en el que resultan afectados datos personales; consentimiento innecesario ahora con la propia LTBG.

Además, no debe olvidarse que, en todo caso, deben respetarse los principios básicos sobre protección de datos; distinguiéndose cuando la información contiene datos de salud (especialmente protegidos) -que, según el art. 15 LTBG, requieren el consentimiento expreso del afectado-; y si los datos no tuvieran ese carácter, en cuyo caso será necesario realizar una ponderación entre el interés público en la divulgación de la información y los derechos de los afectados, en concreto, su derecho a la protección de datos personales (art. 15.3).

En este sentido, en la determinación de la ponderación entre publicidad y privacidad debe considerarse que la categoría de datos especialmente protegidos supone una importante directriz para dilucidar cuando una publicidad inconsentida por la vía del otorgamiento del acceso puede implicar una mayor injerencia en los derechos constitucionales de los afectados, y por ello, debe ser excepcional, sólo justificada por la prevalencia de otro derecho fundamental"[807].

Como señala RAMS RAMOS, en la medida en que estamos ante el "choque" de dos derechos llamados a entrar en conflicto por su ámbito de protección, el de acceso a la información y el derecho a la protección de datos, que se configura como fundamental por el ordenamiento jurídico, la necesaria conciliación de ambos se hace más compleja si

[806] PIÑAR MAÑAS, J.L., *Transparencia, acceso a la información y protección de datos*, *op.cit*, pp. 58-60.

[807] GUICHOT REINA, E., "Principios de la protección de datos: comunicación de datos por las administraciones públicas a sujetos privados (1)", en *Comentario a la Ley Orgánica de Protección de datos de carácter personal*, TRONCOSO REIGADA, A., (Dir.), *op.cit.*, p.4.

cabe; siendo necesario articular " un complicado sistema de equilibrio regulatorio –en el que no se invada la reserva de ley orgánica que la Constitución Española establece– sino también a establecer reglas jurídicas por las que la protección del derecho fundamental no lleve a la necesaria denegación sistemática del derecho de acceso a la información que, aunque no goce de dicha especial protección del ordenamiento jurídico, se ha convertido en un elemento esencial de realización del principio democrático y que, como tal, trasciende la mera satisfacción del derecho subjetivo, para convertirse en piedra angular de un sistema que exige la realización del principio de transparencia como garantía de su funcionamiento democrático"[808].

En los datos meramente identificativos y que no sean especialmente protegidos, la propia LTBG, para resolver la aplicación del derecho de acceso, no establece una regla de exclusión (que si se aplica a los datos especialmente protegidos, ni una regla generalizada de accesibilidad, que se aplica a los datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano); sino que determina que deberá solventarse mediante una ponderación "suficientemente razonada" de los derechos e intereses que intervienen en cada caso concreto; lo que obliga a que la mayor parte de las situaciones de conflicto entre la protección de datos y la transparencia sean resueltas de forma ponderada atendiendo las circunstancias singulares concurrentes en el caso examinado. Debiendo desecharse una resolución que de forma automática otorgue preferencia aplicativa a un derecho frente a otro[809].

La información solicitada debe comunicarse con carácter general si se cumplen las condiciones establecidas, siendo la excepción la denegación de la misma. Así, deben cumplirse los siguientes requisitos o condiciones[810]:

-Debe llevarse a cabo, como veíamos, una previa ponderación suficiente y razonada de los intereses en juego (*fair balanced*), valorando en concreto la incidencia el interés público y los derechos de los afectados, cuyos datos aparezcan en la información solicitada y, especialmente, su derecho a la protección de datos personales. Lo que se

[808] RAMS RAMOS, L., "El derecho fundamental a la protección de datos de carácter personal como límite ¿(in)franqueable? para la transparencia administrativa", Estudios de Deusto, Vol. 66/2, julio-diciembre 2018, págs. 119-152. Accesible en: http://www.revista-estudios.deusto.es/.
[809] CTPD Andalucía, RES/042/2016, de 22 de junio.
[810] Art. 15.3 LTBG.

pondrá de manifiesto en la resolución administrativa comunicada al solicitante y demás interesados.

-Apertura de un trámite de audiencia (trámite fundamental) para que en quince días el titular afectado presente las alegaciones oportunas, conforme al art. 19.3 LTBG; las cuales serán tomadas en consideración por el sujeto público dentro del proceso de ponderación de intereses. En el supuesto de que dichas alegaciones incorporen una oposición del titular del dato podrá procederse, sin embargo, al suministro de la información al solicitante por parte del órgano administrativo; aunque deberá tenerse en cuenta para ponderarlo, debiendo motivar el acceso concedido (art. 20.2). No obstante, la entrega de la información deberá esperar a que finalice el plazo para interponer recurso contencioso-administrativo (dos meses), o bien, éste haya sido resuelto en el sentido de conceder el acceso (art. 22.2). Esta misma cautela será aplicable cuando se realice una reclamación ante el CTBG (nacional o autonómico) sobre la base de la oposición del tercero titular de los datos.

Además, esta ponderación singular de intereses, que necesariamente habrá de considerar los criterios propios de la protección de datos "tomará particularmente en consideración los siguientes criterios" (entre otros, cabe interpretar[811]), previstos en el apartado 3º[812]:

[811] En este sentido, a la hora de determinar la aplicación prevalente de la normativa sobre protección de datos o la propia de la LTBG, habría que considerar, además de los criterios previstos en la LTBG, como se lleva a cabo el procedimiento de ponderación por el Tribunal Europeo de Derechos Humanos basado en un procedimiento con tres etapas diferenciadas: 1º, si existe injerencia en el derecho a la vida privada, y si está prevista en la ley y legítima; 2º ponderación de si la medida estatal está amparada por el Derecho, y 3º un juicio proporcionalidad a la vista del principio de necesidad propio de una sociedad democrática: Martínez Gutiérrez, R., en *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información*, VALERO TORRIJOS, J. FERNÁNDEZ SALMERÓN (coords.), Thompson Reuters, Pamplona, 204, pp.26-261.

[812] Art. 15.3. LTBG:

"a) El menor perjuicio a los afectados, derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

a) El transcurso de los plazos de la Ley de Patrimonio Histórico Español (LPHE), a los que remite la propia LTBG: 25 años de la muerte del titular del dato personal y 50 años desde la fecha de suscripción del documento[813].

b) Que el solicitante justifique su solicitud en el ejercicio de un derecho, aplicándose para el ejercicio de cualquier tipo de derecho subjetivo (fundamental, legal o contractual). Se exige que el solicitante motive las razones de solicitud de la información sobre las que no debe entrar a valor el órgano competente, que debe limitarse a comprobar que el solicitante es titular del derecho invocado y la relación existente con la información solicitada[814].

c) Que el solicitante tenga la condición de investigador (o bien realizar funciones investigadoras) y que la solicitud se base en fines históricos, científicos o estadísticos[815]. Ante la múltiple casuística de personas que pueden tener la condición de investigador, que incluiría no solamente a quienes profesionalmente se dediquen a ello, sino a otro tipo de personas, como becarios y universitarios que también realizan actividades investigadoras, señala FERNÁNDEZ RAMOS[816], que, además de la necesaria motivación del solicitante del objeto de la solicitud, debería considerarse el

[813] Conforme al art. 57.1:
"La consulta de los documentos constitutivos del Patrimonio Documental Español a que se refiere el artículo 49.2 se atendrá a las siguientes reglas:
c) *Los documentos que contengan datos personales* de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos".

[814] Como explicara magistralmente la STS de 30-3-1999: "El Abogado del Estado pretende, en síntesis, que condicionemos el reconocimiento del derecho a obtener el acceso al expediente a la real existencia de los presupuestos necesarios para el ejercicio del derecho de reversión sobre cuya procedencia el recurrente precisamente pretende informarse. Si accediéramos a esta pretensión estaríamos vinculando, del modo que hemos considerado incompatible con el principio constitucional de acceso a los registros públicos, la posibilidad de obtener la información útil para ponderar las posibilidades jurídicas de ejercicio de una pretensión al parecer administrativo sobre la efectiva titularidad del derecho o del interés legítimo hacia el conocimiento de cuyos presupuestos van dirigidas las averiguaciones. Con ello resultaría sacrificada la función instrumental de la información en aras del criterio de fondo de la Administración sobre el objeto a que la misma se refiere y, de este modo, al privar al interesado de los elementos para tomar por sí mismo su decisión y devenir así inútil el derecho de acceso a los archivos y registros públicos (suplantado por el parecer de la Administración sobre la posible utilidad de su resultado), se vulneraría su núcleo esencial, no dependiente de la configuración legal de su ejercicio".

[815] La LOPD se refería a estos fines cualificados "históricos, científicos o estadísticos", en el art. 4.2., que consideran que no son incompatibles con las finalidades para las que se recogen; y en el art. 11.2.d) al excluir de la necesidad de consentimiento del afectado en la cesión de datos entre Administraciones públicas y que tenga por objeto "el tratamiento posterior de los datos con fines históricos, estadísticos o científicos".

[816] FERNÁNDEZ RAMOS, *Acceso a la información pública versus protección de datos personales*, *Op.cit*.

concepto de investigador en un aspecto esencialmente funcional (básicamente, es investigador quien investiga), que se acomoda mejor con su naturaleza de derecho fundamental, previsto en el art. 20.1. b) CE[817].

d) Podrá denegarse motivadamente la información, cuando los datos puedan afectar a la intimidad y a la seguridad; por tanto, que contengan alusiones a personas identificadas o identificables, cuya protección de debe prevalecer sobre el acceso; se refieren, entre otros supuestos, a menores de edad, en cuyo caso habrá de considerarse la promoción en todo caso del interés del menor[818]. Supone un conjunto amplio de informaciones personales caracterizado por una elevada indeterminación, situándose en una categoría intermedia entre los datos especialmente protegidos y los meramente identificativos[819]. Podrá denegarse, igualmente, cuando en el acceso exista oposición de un tercero.

No obstante, "(…) *no será necesario considerar los anteriores supuestos del art. 15.3 si se utiliza la técnica de la previa disociación de los datos personales de forma que se impida la identificación de los titulares afectados*" (art. 15.4).

Por ello, tratándose de la concesión del acceso parcial mediante seudononimización o disociación, deberá dictarse una resolución motivada, en aplicación del art. 16, que, aunque referido al acceso parcial de los límites del art. 14, debe entenderse también aplicable a los supuestos de limitación de la información por la existencia de datos personales necesitados de protección[820].

[817] Anteriormente a la LTBG, el Real Decreto 1708/2011, por el que se establece el sistema español de archivos de la Administración General del Estado y sus organismos públicos y su régimen de acceso, establece en su art. 28:
"(…)3. El acceso a documentos que contengan datos nominativos o meramente identificativos de las personas que no afecten a su seguridad o su intimidad, será posible cuando el titular de los mismos haya fallecido o cuando el solicitante acredite la existencia de un interés legítimo en el acceso.
A estos efectos, se entenderá que poseen interés legítimo quienes soliciten el acceso para el ejercicio de sus derechos y los investigadores que acrediten que el acceso se produce con una finalidad histórica, científica o estadística".

[818] La Ley Orgánica de Protección Jurídica del Menor establece la primacía del interés del menor sobre cualquier otro interés legítimo que pudiera concurrir. No obstante, la información podrá facilitarse si se garantiza su carácter anónimo (Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno de Cataluña, art. 21.3).

[819] FÉRNANDEZ RAMOS, *Acceso a la información pública versus protección de datos personales*, *op.cit*., p. 24.

[820] ENÉRIZ OLAECHEA J., *op.cit.*, pp. 6 y ss.

Además, a partir de las resoluciones del CTBG (nacional y autonómicos) y de la AEP, pueden extraerse otros criterios interpretativos en la resolución de la solicitud de acceso:

- Así, el criterio subjetivo de la mayor relevancia pública del titular de los datos, en la medida de que no debe tener igual relevancia una información que afecte a una persona de niveles inferiores, o que incluso no participa de las funciones públicas, que, si afecta a un alto directivo, cargo público o de confianza; sobre el cual, deben favorecerse el acceso de datos identificativos de quienes desarrollan funciones que incidan en el proceso de toma de decisiones de la entidad[821].

- Otro criterio interpretativo, sería el de ser titular de un interés legítimo, que tiene un contenido más amplio que el referido al ejercicio de un derecho, previsto en la LTBG. Así, hemos visto como, de una parte, no será necesario el consentimiento del afectado cuando "(…) *el tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado en dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el art. 1 LOPD*"[822] y de otra, el RGPD considera lícito el tratamiento cuando "(…) *sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales*"(art. 6.f)).

Como ejemplos de la utilización de este criterio, podemos señalar el ámbito de los procedimientos de concurrencia competitiva, sobre el que se han pronunciado distintas resoluciones del CTBG y la AEPD, en las que se admitía que las Administraciones públicas a fin de comprobar la imparcialidad del procedimiento deben suministrar a los interesados la información solicitada del proceso selectivo, que incluya los datos personales de terceros participantes en la selección[823].

[821] Criterio interpretativo conjunto del CTBG y AEPD, CI/001/2015, de 23 de marzo de 2015.

[822] Art. 10.2.a) RLOPD.

[823] En este sentido, la Sentencia de 26 de abril de 2012 de la Audiencia Nacional (Sección Primera de la Sala de lo Contencioso-Administrativo), señaló lo siguiente: (…. Es cierto que la Ley Orgánica 15/1999 no recoge expresamente exenciones o excepciones al régimen de tratamiento de datos personales en ella contenida con fundamento en las garantías de transparencia de los procesos competitivos por lo que será preciso ponderar los intereses en conflicto para poder determinar cuál de ellos debe prevalecer. Efectuada

Por ello, en el supuesto de que la información solicitada contribuya de una manera decisiva a la finalidad de un mejor conocimiento de los criterios de organización y funcionamiento de las instituciones o la asignación de recursos, se trataría de una información que prevalecería sobre los posibles derechos de los interesados.

En este sentido, el supuesto clásico de solicitud de información derivada de un procedimiento de selección de personal, en el ámbito público, sería el principio de igualdad el que, de modo prevalente, ampararía la comunicación de datos personales de los seleccionados, siendo intrascendente que se publiquen los datos de los candidatos no seleccionados, justificando así su protección[824].

Sin embargo, tratándose de la selección de personal funcionario a través de un procedimiento de libre designación, en el que se pretende acceder a la documentación relativa al concurso, sería necesario que, existiendo datos personales, se pondere la vulneración de derechos de los distintos concursantes, de forma que debe restringirse el acceso a los currículos de los aspirantes y cualquier otro dato que contenga información personal; excepto que la solicitud se refiera al adjudicatario del puesto, ya que: "A nuestro entender, el interés público en la divulgación de información relativa a una persona nombrada para un puesto no directivo de libre designación de nivel 30, 29 o 28, o equivalentes, debe prevalecer, con carácter general, sobre su interés individual en la preservación de la intimidad y los datos de carácter personal. […] Por otra parte, el hecho de que únicamente se permita el acceso al currículo del adjudicatario desvanece o aminora sustancialmente el riesgo de que se afecte a la concurrencia en futuras convocatorias. Así las cosas, este Consejo considera que la ciudadanía tiene derecho a conocer, por vía del derecho de acceso, qué currículo tiene un adjudicatario de un puesto de libre designación con un nivel 28, 29 o 30; adjudicación que, no olvidemos, tiene carácter discrecional".

Aunque, no deben ser objeto de comunicación datos meramente personales, como el DNI, fecha de nacimiento, domicilio, teléfono, correo electrónico personal, datos familiares, además de, por supuesto, cualquier otro dato especialmente protegido, conforme a la normativa sobre protección de datos. Por todo ello, ha de prevalecer el interés público en

dicha ponderación, y valorando las circunstancias que aquí concurren, es claro para este Tribunal que debe prevalecer en este caso la garantía de publicidad y transparencia del proceso competitivo sobre el derecho a la protección de datos).

[824] CPPD Andalucía, RES/32/2016, de 1 de julio.

conocer el perfil curricular del adjudicatario de un puesto de libre designación, disociando los referidos datos de carácter personal[825].

En todo caso, la información resultante del derecho de acceso deberá someterse para su tratamiento posterior a la normativa sobre protección de datos, como señala innecesariamente el art. 15.5 LTBG, considerando el contenido amplio del término tratamiento del art. 4.2. RGPD, y a la vista del principio de finalidad y demás principios que rigen la protección de datos.

Relacionado con los deberes de publicidad activa, estos deberes afectan al derecho de acceso a la información pública de una forma positiva y directa, en el sentido de que la información comprensiva de datos personales (dejando a salvo los datos especialmente protegidos, art 5.3. LTBG) resulta accesible cuando es la ley la que ordena su publicación; de forma que, si no fuera publicada la información, permitiría solicitar su acceso sin necesidad de ponderación alguna. Es el caso de la propia LTBG, que su art. 1.g) obliga a la publicación de las resoluciones de reconocimiento o autorización de compatibilidad de los empleados públicos; de lo que resulta que dichas resoluciones deben ser accesibles no sólo en lo que evidentemente es objeto de publicación sino del resto de contenido, aunque contenga datos personales de los afectados[826].

Si la información solicitada está afectada por un contenido sanitario o de salud, podemos encontrar los siguientes ejemplos de criterios interpretativos:

Tratándose del criterio interpretativo relacionado sobre información relativa a las agendas de los responsables públicos[827], se solicita el acceso sobre la información de las reuniones y de la identificación de los asistentes a las mismas, celebradas por miembros del Gobierno, altos cargos o empleados públicos.

Esta información sobre la agenda de los organismos públicos también puede llevar a que el acceso recaiga sobre datos de salud cuando las reuniones de sus miembros estén formadas por asociaciones de enfermos de una determinada dolencia, discapacidad, colectivos de una determinada etnia o personas de una determinada preferencia sexual.

825 CTPD Andalucía, RES/35/2017, de 15 de marzo de 2017.

826 Así, el CTBG ha entendido que es posible acceder a los datos de identificación de los destinatarios de las resoluciones de incompatibilidad. R/0432/2016, de 22 de diciembre de 2016

827 CI/002/2016 del CTBG.

En estos casos, procede conceder el acceso si ha existido consentimiento expreso o exista una ley que habilite para conceder el acceso.

Tratándose de datos sensibles derivados del conocimiento de otros documentos, por ejemplo, declaración patrimonial de altos cargos, la R/0051/2016, resolvió un caso que tenía por objeto estudiar una denegación parcial de acceso a la información por parte de la Oficina de Conflictos de Intereses del MINHAP. El solicitante reclamaba acceso a la información sobre la declaración de actividades a la toma de posesión, declaración de bienes a la toma de posesión y declaraciones anuales para los años 2012, 2013 y 2014 del presidente y sus ministros. La denegación del CTBG se basó en el carácter reservado de dichas declaraciones, así como que conceder el acceso a las mismas supondría una vulneración al derecho a la protección de datos.

Asimismo, considera que dar acceso a esta información conlleva al conocimiento y potencial vulneración de otros datos especialmente protegidos, como la orientación sexual (en el supuesto de matrimonio con una persona del mismo sexo), la ideología (si el alto cargo contribuye a organizaciones políticas), la religión (si el declarante optara por contribuir a la iglesia católica), la salud (en caso de que tanto el alto cargo o alguno de sus familiares directos padezcan algún tipo de discapacidad), así como los datos identificativos tanto del cónyuge como de sus descendientes. Por todo ello, el CTBG concluye que existen datos especialmente protegidos y que se encuentran en la esfera íntima, personal y familiar de los titulares de los datos, por lo que no puede divulgarse dicha información sin vulnerar la normativa vigente.

La AEPD, en su informe 0178/2014, contempla las situaciones derivadas de la publicación de los datos de beneficiarios de ayudas a personas con discapacidad, sin que se especifique el tipo de discapacidad. Así, entiende que, la publicación de la condición de discapacidad de las personas que reciban alguna subvención o beneficio, de conformidad con lo que establece el artículo 8.1.c) de la LTAIBG, se trata de datos relacionados a la salud de una persona, según el artículo 7 de la LOPD; a cuyo efecto, se aplica lo dispuesto en el artículo 5.3 y artículo 15 de la LTAIBG, así como las reglas del artículo 7 de la LOPD. Señalando que lo procedente es que la publicación –ya sea en un tablón de anuncios o sitio web- se lleve a cabo previa disociación de los datos personales relacionados con las subvenciones de forma que no sea identificable el beneficiario. Añade, además, que, para estos casos, el dato especialmente protegido no es el tipo de

discapacidad, sino la existencia de la misma por lo que en todo caso debe procederse con la disociación.

3.4. PROCESO PARA RESOLVER LAS SOLICITUDES DE ACCESO

Siguiendo el criterio del CTBG (CI/002/2015), el proceso de aplicación de la LTBG debe comprender las siguientes etapas o fases sucesivas:

I. Valorar si la información solicitada o sometida a publicidad activa contiene o no datos de carácter personal, entendiéndose por éstos los definidos en el artículo 3 de la LOPD.

II. En caso afirmativo, valorar si los datos son o no datos especialmente protegidos en los términos del artículo 7 de la LOPD, esto es:

a) Datos reveladores de la ideología, afiliación sindical, religión y creencias; En este caso la información se podrá facilitar cuando se cuente con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso;

b) Datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual. Se podrán facilitar los datos cuando se cuente con el consentimiento expreso del afectado o estuviera amparado por una norma con rango de Ley;

y c) Datos de carácter personal relativos a la comisión de infracciones penales o administrativas. Se podrá facilitar siempre que las correspondientes infracciones penales o administrativas no conlleven la amonestación pública al infractor, cuando se cuente con el consentimiento expreso del afectado o estuviera amparado por una norma con rango de Ley.

III. Si los datos de carácter personal contenidos en la información no fueran datos especialmente protegidos, habría que valorar:

a) si son exclusivamente datos meramente identificativos relacionados con la organización, el funcionamiento o la actividad pública del órgano o entidad correspondiente. Si los datos contendidos son exclusivamente identificativos relacionados con la organización, el funcionamiento o la actividad pública del órgano

o entidad, la información se publicará o facilitará con carácter general, salvo que en el caso concreto prevalezca la protección de datos personales y otros derechos constitucionalmente protegidos sobre el interés público en la divulgación.

b) si no fueran meramente identificativos y relacionados con la organización, el funcionamiento o la actividad pública del órgano o no lo fueran exclusivamente, procede efectuar la ponderación prevista en el artículo 15 número 3 de la LTBG.

Por tanto, en líneas generales, el proceso de aplicación de la normativa de protección a la solicitud de información pública transcurre a través de las siguientes etapas:

1º.- Valoración de si la información solicitada contiene o no datos personales.

2º.- Si contiene datos personales y se trata de datos de salud (son especialmente protegidos) no debe accederse a la solicitud salvo consentimiento expreso del afectado o que exista un amparo legal que lo propicie.

3º.- Si los datos no fueran especialmente protegidos podrá disociarse la información si el solicitante quiere.

4º.- Si se trata de datos únicamente identificativos y relacionados con la actividad y organización del órgano, se accederá a la solicitud como regla general, salvo que en el caso concreto prevalezca la protección de datos personales y otros derechos constitucionalmente protegidos sobre el interés público en la divulgación.

5º.- Si se trata de datos distintos a los previstos en el apartado anterior habrá que proceder a su valoración de acuerdo con los criterios ponderativos expresados.

CONCLUSIONES

CONCLUSIONES

PRIMERA. CONTENIDO DE LA PROTECCIÓN DE DATOS PERSONALES

La existencia de la protección de datos se debe a la necesidad de dar protección a la intimidad personal y a la información personal (sea íntima o no, e incluya datos públicos), como concepto que incluye lo relativo a la vida personal y familiar de una persona, en línea con la idea de "*privacy"* anglosajona. Y así, ante esta necesidad acrecentada de protección por el nacimiento de las nuevas tecnologías y el uso de la informática, como mecanismo de respuesta constitucional y de defensa y protección de la dignidad y los derechos de la persona amenazados, surgen dos instrumentos de tutela jurídica: la libertad informática, cuyo objeto es el control del tratamiento automatizado de datos, y el derecho a la protección de datos personales; los cuales vendrían a coexistir y complementar al derecho a la intimidad.

Así, este derecho a la autodeterminación informativa o de protección de datos, tuvo su reconocimiento y garantía gracias al trascendente papel que ha jugado el TEDH y su sentencia en el caso *Leander* que supuso el reconocimiento de este derecho como parte del derecho a la vida privada reconocido en el art. 8 CEDH. España, ha sido un país pionero en el reconocimiento constitucional de este derecho como derecho fundamental (art. 18.4) y en las SSTC 290/2000 y 292/2000, de 30 de noviembre.

El derecho a la protección de datos, cuyo objeto no es únicamente la protección de la intimidad sino cualquier tipo de dato personal que concierne a su titular, se extiende a toda persona y se manifiesta atribuyéndola un poder de disposición y control de todo aquello que forma su espacio más privado e íntimo en cuanto tiene repercusión externa (sus datos personales); facultades que le permiten decidir libremente qué hacer con sus datos: si proporcionarlos o no a un tercero, o decidiendo cuales puede recabar éste; y estar informado sobre quien posee sus datos y con qué finalidad, pudiendo oponerse a ello. Y este control (en poder de su titular) para el tratamiento de sus datos por terceros se

manifiesta a través de su consentimiento expreso y, a falta de este, en la autorización o habilitación legal.

Esta protección sobre los datos personales que brinda el ordenamiento jurídico se articula mediante garantías en favor del titular de los datos; las cuales se materializan a través del cumplimiento de deberes jurídicos impuestos a los terceros que utilizan los datos personales, destinados a conocer la finalidad o propósito por el que se recaban y su utilización posterior. Así, esta normativa sobre protección de datos se ha visto modificada recientemente, por cuanto tras vinculación normativa directa, el 25 de mayo de 2018, del RGPD, se produjo la publicación de la LOPDGGD, entrando en vigor el 7 de diciembre de 2018; constituyendo ambos textos legales el conjunto normativo aplicable en la materia. Ello, sin olvidar como la doctrina y jurisprudencia de la etapa anterior (LOPD y su Reglamento), junto a las resoluciones de la AEPD y agencias autonómicas, sentaron las bases del actual sistema de protección de datos; por lo que su valor aplicativo e interpretativo es innegable.

SEGUNDA. GARANTÍAS DEL SISTEMA DE PROTECCIÓN DE DATOS: LAS SANCIONES

El sistema de protección de datos personales necesita, para su cumplimiento y, por ello, su adecuado funcionamiento por sus destinatarios, estar apoyado por un sistema sancionador que, como proclama el RGPD, tenga un carácter disuasorio, y en el que la prioridad no es la imposición de sanciones, sino trabajar desde el cumplimiento adecuado y racional de las normas sobre protección de datos; previniendo las posibles situaciones de infracción de los derechos en él reconocidos.

Frente al RGPD, que se limita a definir casi en exclusiva el régimen jurídico aplicable, la regulación del régimen sancionador prevista en la LOPDGDD es más precisa y completa, al establecer cuestiones como la prescripción ignoradas por el Reglamento. Así, el sistema cuenta con la imposición de multas administrativas (pudiendo llegar a los veinte millones o el 4% del volumen de negocio de la empresa), como forma de imposición de las sanciones, así como de las medidas previstas en el art. 58 RGPD, cuya competencia corresponde a las autoridades nacionales y autonómicas de control.

Se consideran sanciones muy graves las derivadas del incumplimiento de las normas; como el tratamiento de datos de salud (y, de los encuadrados en las categorías especiales) fuera de los casos habilitados o excepcionados en la LOPDGDD, así como otros incumplimientos sustanciales, como la vulneración de los principios y garantías fijados en el Reglamento o el tratamiento sin base habilitante, al que se asimila la prestación del consentimiento inválido. Las infracciones graves derivan de la violación de los derechos de las personas derivadas de la falta de previsión o de adopción de las medidas previstas para garantizar dichos derechos; como las necesarias para llevar a cabo un adecuado tratamiento de datos.

TERCERA. CONTENIDO DE DATOS DE SALUD EN DOCUMENTACIÓN SANITARIA

En el caso de datos personales de contenido sanitario o de salud (aquellos relacionados con la salud -estado de salud- de una persona), la garantía que supone para su titular la protección de sus datos que le brinda el ordenamiento jurídico se traslada al ámbito de la salud, mediante un reforzamiento de la protección normal propia de estos datos sensibles (y de la categoría especial de datos a la que pertenecen), y cuyo contenido se ha ampliado (tanto por el RGPD como por la LOPDGDD) incluyendo los datos genéticos como datos de salud, además de los biométricos. Y esta garantía se materializa básicamente mediante la prohibición de su tratamiento como regla general.

Al mismo tiempo, se produce la confluencia de dos tipos de ordenamientos: el general, propio de la protección de datos personales, y el específico, regulador de la actividad sanitaria o de salud pública, en el que los datos de salud cumplen una finalidad fundamental: servir para una mejor atención sanitaria del paciente. De ahí, que todo el entramado jurídico de la protección de datos no pueda trasladarse directamente al ámbito sanitario sin considerar las regulaciones específicas sanitarias; de forma que ambos ordenamientos habrán de aplicarse de forma congeniada, siendo imprescindible realizar una interpretación amplia y generosa de la normativa y principios de la protección de datos, que no entorpezca la necesaria asistencia sanitaria al paciente, que debe ser el objetivo prioritario.

Partiendo de la información clínica, como conjunto de datos relacionados con el estado de salud de una persona, que se contienen en un soporte en el que se incluyen todos los datos asistenciales de un paciente (documentación clínica), los datos de salud pueden encontrarse en distintos documentos clínicos: básicamente la Historia Clínica (HC), como documento clínico esencial para la atención del paciente y de la asistencia sanitaria en general, comprensivo de información sanitaria y de otra complementaria que forma parte del respeto a la vida privada y familiar; merecedora, por ello, de un especial régimen de protección.

A esta documentación habría que añadir, además de las instrucciones previas, otros documentos regulados fuera de la LBAP, como la receta (tanto en papel como electrónica), las órdenes de dispensación de medicamentos y la tarjeta sanitaria; todos ellos, comprensivos de información/datos de contenido sanitario y, por tanto, necesitados de una especial protección. Junto a la información asistencial o clínica, existe, la información sanitaria (en sentido amplio), también susceptible de contener datos de salud, y, por tanto, merecedora de protección, y a la que es posible acceder por la vía de la publicidad activa o pasiva (derecho de acceso).

CUARTA. TRATAMIENTO Y SEGURIDAD DE LOS DATOS DE SALUD

Para que la protección de datos personales despliegue sus efectos, es preciso que se realice cualquier tipo de intervención (tratamiento, en sentido amplio) realizada sobre cualquier información que permite identificar o pueden hacerla identificable con una persona física (persona concernida), al margen de la forma utilizada. Y esta protección se lleva a cabo a través de los preceptos incluidos en la normativa aplicable (RGPD y LOPDGDD) y de los principios básicos del tratamiento de datos. Estos principios, reconocidos inicialmente en el Convenio 108 y en la CDFUE y, posteriormente ampliados por la Directiva 95/46/CE y por el RGPD -que distingue entre los que se aplican a todo el tratamiento y los que legitiman dicho tratamiento-, siguen siendo trascendentales en el tratamiento de datos personales al inspirar toda la regulación de la protección de datos; por lo que forman parte del contenido esencial del derecho a la protección de datos.

La LOPD (partiendo de la denominada calidad de los datos en que se basa el Convenio) acogía el principio de calidad de los datos como uno de sus principios básicos, que venía a englobar tres mandatos esenciales:

a) que los datos sólo podrán recabarse cuando sean adecuados, pertinentes y no excesivos en relación con la finalidad para la que se hayan obtenido, y sólo deberán tratarse si la finalidad del tratamiento no pudiera conseguirse razonablemente por otros medios; que, en el ámbito de la asistencia sanitaria significa que sólo deben solicitarse los que estrictamente sean necesarios para la atención al paciente, debiendo existir proporcionalidad entre el acceso a los datos de la HC con su utilización en una estricta función asistencial o, tratándose de otros accesos autorizados, la exclusiva función judicial;

b) que los datos sólo podrán utilizarse para las finalidades, determinadas y legítimas del responsable del tratamiento para las que se hayan obtenido, sin que puedan ser utilizados para otros fines incompatibles con éstos (principio de finalidad, trascendental para garantizar que el tratamiento respeta los derechos fundamentales del titular); considerando la necesidad de que exista un consentimiento informado del titular, manifestado de forma expresa e inequívoca, una vez ha sido informado de forma comprensible de la existencia del fichero, de su titular y de la finalidad del destino de los datos; o bien se trate de otra base legítima distinta habilitante del tratamiento;

y, c) además, deben ser exactos y actualizados; exigencia de indudable trascendencia en el ámbito del tratamiento de la salud ante la necesidad de que los datos clínicos de los pacientes sean veraces y actuales; además, deben de mantenerse durante el tiempo necesario para cumplir los fines del tratamiento; que, nuevamente, en el ámbito de la atención sanitaria, resulta necesario excepcionar ante determinados tratamientos crónicos que exigen una continuidad de información; igualmente, deben recabarse de forma clara y transparente, con métodos no fraudulentos, desleales e ilícitos.

Por último, el RGPD (como su novedad más importante), abandonando el anterior sistema de seguridad por capas, centrado en el control del cumplimiento de las normas, se centra en un nuevo sistema de responsabilidad basado en la responsabilidad proactiva y preventiva, derivada de la anticipación y evaluación anticipada del riesgo que pudiera producir el tratamiento de datos; manteniendo la protección de la privacidad durante la

existencia de los datos personales e integrada en los propios sistemas organizativos y de gestión (*Privacy by Design y Privacy by Default*). De esta forma, como principio de tratamiento y obligación derivada del RGPD, debe garantizarse, por parte del responsable y el encargado del tratamiento, una seguridad adecuada para preservar la integridad de los datos, mediante la puesta en marcha de medidas organizativas y de seguridad adaptadas al tipo de riesgo expuesto (como el mínimo tratamiento de datos y su seudonimización); por lo que, tratándose de datos de máximo riesgo para la privacidad, como son los datos de salud, habrán de implementar medidas que se ajusten a ese riesgo, además de realizar una Evaluación de impacto (EIPD) previa a la realización del tratamiento de estos datos, que sólo afectará a los datos clínicos de la HC y no a los de carácter personal en ella incluidos, en los que el posible riesgo a acaecer tendría otro alcance.

QUINTA. DERECHOS DE LOS TITULARES DE DATOS DE SALUD: ACCESO TANTO NACIONAL COMO TRANSFRONTERIZO A LA HC

Junto a los principios aplicables al tratamiento de datos, la normativa sobre la materia reconoce a los titulares de datos personales un conjunto de derechos de carácter personalísimo que se pueden ejercer libremente frente al responsable del tratamiento, mediante los cuales su titular dispone de un poder de control de los datos personales a fin de garantizar el respeto a esta normativa en el tratamiento de datos; y este poder de control se materializa poniendo a disposición del titular de los datos la posibilidad de ejercitar un conjunto de derechos que vienen a reforzar esa posición de control de los datos, reconocidos en los arts.16 a 22 RGPD. Así, el titular de los datos, a fin de comprobar si sus datos están siendo tratados lícitamente, puede acceder a los mismos solicitando del responsable del tratamiento información sobre cómo se realiza su tratamiento y su comunicación, en su caso, a un tercero.

Tras la aprobación del RGPD y de la LOPDGDD, los iniciales derechos ARCO se han visto ampliados con el derecho a la portabilidad, al Olvido y a la limitación del tratamiento; de forma que ahora estamos ante los denominados ARCO-POL, cuyo ejercicio debe llevarse a cabo conforme al principio de transparencia e información (artículo 11 LOPDGDD).

En el ámbito sanitario, podemos encontrarnos ante el acceso del paciente a su Historia Clínica (HC), que estará limitado por: no poder perjudicar derechos confidenciales de terceros y por no poder acceder a las anotaciones subjetivas del médico, ni cuando exista una necesidad terapéutica del paciente.

Junto al paciente, otros profesionales, tanto sanitarios como no sanitarios pueden acceder a la HC, debiendo respetar la confidencialidad de sus datos, sin necesidad de consentimiento del afectado, como legitimación válida derivada de la base jurídica proporcionada por el RGPD: tratándose de centros sanitario privados, el acceso deriva del cumplimiento de una obligación contractual (art. 6.1.b); cumplimiento de una obligación legal (art. 6.1.c)), o, en su caso, proteger intereses vitales o esenciales del interesado, o de otra persona física (cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente), lo que permite que, en base a razones conjuntas de interés público en el ámbito de la salud pública, pueda justificarse un tratamiento excepcional de datos en situaciones, como la presente, de emergencia epidemiológica (art. 6.1.d) y art. 45 RGPD.

Además, es preciso que el tratamiento de datos (en este caso el acceso a la HC) se realice, tanto en interés público esencial (apartado g), como cualificado (aparto i), previsto para situaciones de salud pública (y que incluye todos los elementos relacionados con la protección de la salud (art. 9.2 RGPD), como la protección frente a amenazas transfronterizas graves para la salud, derivada del reconocimiento del derecho a la asistencia sanitaria a pacientes transfronterizos (reconocida por la Directiva 2011/24/UE), pero aplicable sólo a prestaciones de seguridad social, y que debe respetar el derecho a la intimidad en el tratamiento de datos de salud realizado conforme a la normativa sobre protección de datos. Esta asistencia sanitaria transfronteriza, segura y de calidad, habida cuenta de las diferentes regulaciones de los sistemas sanitarios de los países miembros, debe tender a homogeneizarse a través de la interoperabilidad de los distintos sistemas tecnológicos de *eHealt*; permitiendo eliminar obstáculos a la asistencia sanitaria y posibles riesgos para los pacientes.

SEXTA. TÍTULOS JURÍDICOS HABILITANTES DEL ACCESO A LOS DATOS DE SALUD

La excepción a la prohibición de tratamiento de, entre otros, la salud, la sanidad pública y la gestión de la asistencia sanitaria, con fines de interés público y, siempre que se den las garantías de protección de datos y de otros derechos fundamentales, se encuentra amparada en las leyes sanitarias: LGS, Ley de Medidas Especiales en Materia de Salud Pública, LBAP, Ley de Cohesión del Sistema Nacional de Salud, Ley General de Salud Pública y Ley de Investigación Biomédica, conforme a la Disp.Adic,17ª LPDGDD; dando así respuesta a la exigencia del RGPD (Considerando 52), de que dicha prohibición esté autorizada en una norma nacional o europea.

Así, los profesionales sanitarios vinculados directamente al paciente podrán acceder a la HC sin consentimiento expreso del paciente, en cumplimiento de la finalidad de prevención, diagnóstico y asistencia sanitaria, como excepción, de carácter restrictivo, a la prohibición general de tratamiento de los datos de salud, limitada a un acceso a lo estrictamente necesario para el tratamiento del paciente; lo que constituye, no una cesión de datos, sino un acceso legitimado por la exclusiva finalidad asistencial del paciente.

Al mismo tiempo, otros profesionales no sanitarios que colaboran en la gestión sanitaria pueden acceder a la HC, vinculados, igualmente, con la obligación de confidencialidad respecto de los datos personales del paciente, debiendo guardar el necesario secreto de los mismos, amparado en la normativa sanitaria (LBAP, art. 16).

Es posible, además, que, derivado de esta habilitación legal, terceros autorizados puedan acceder válidamente a la HC de un paciente para finalidades diversas, no asistenciales, respetando estrictamente una proporcionalidad ajustada a los fines para los que se accede. Se incluye así: el acceso realizado por las Administraciones Públicas sanitarias (Ley de Cohesión); el propio acceso de la inspección sanitaria, debidamente acreditada (LBAP); el que pueden llevar a cabo Mutualidades y Compañías aseguradoras (Ley de Contrato del Seguro); el realizado con fines judiciales, epidemiológicos (cuando sea necesario acceder a los datos de los pacientes para la prevención de un riesgo o peligro grave para la salud de la población); y el derivado de salud pública, e investigación (Ley de Investigación Biomédica), que exige que existan garantías de los derechos y libertades afectados a través de medidas de seguridad (como la seudonimización, que hace que los

datos no pueden identificarse con su titular sin que se añada nueva información), con separación de datos personales de los clínicos del paciente (LBAP, art. 16).

A propósito del acceso de datos de salud pública, la declaración del estado de alarma (que no implica suspensión de derechos) como consecuencia de la desgraciada epidemia que padecemos actualmente ha puesto de manifiesto la necesidad de que, pese a estar en estas circunstancias extraordinarias, se sigan respetando los derechos y garantías de los afectados, en el tratamiento de datos, en especial, del principio de minimización de datos, de forma que los datos habrán de ser exclusivamente los limitados a los necesarios para la finalidad pretendida: exclusivamente el control de la epidemia; como la utilización de técnicas de geolocalización a través de dispositivos móviles que puedan emitir avisos (anónimos) de afectación por el Coronavirus.

SÉPTIMA. DERECHOS ESPECÍFICOS DE LOS TITULARES DE DATOS DE SALUD

El titular de los datos podrá solicitar del responsable del tratamiento que se rectifiquen o supriman aquellos datos que no cumplan con la normativa sobre protección de datos o sean inexactos o incorrectos; pudiendo, además, solicitar su cancelación (y posterior bloqueo) si fueran inadecuados o excesivos, y oponerse a que sus datos sean tratados en base a una misión de interés público o en interés legítimo, incluido la elaboración de perfiles, así como como cuando tenga una finalidad de mercadotecnia (pudiendo solicitar la suspensión del tratamiento).

Situándonos en el ámbito sanitario, partiendo del carácter muy restrictivo que tienen las excepciones a la prohibición de tratamiento de los datos de especial protección, corresponde de forma exclusiva al profesional sanitario vinculado al paciente determinar concretamente que datos deben ser objeto de supresión; y ello, sobre la base de que los datos de salud nunca se transforman en impertinentes o innecesarios e inadecuados, debido a la necesidad de utilidad continuada que tienen estos datos para la atención sanitaria de los pacientes y, más, si se tratara de patologías cronificadas que exigen un continúo acceso a los datos de una HC actualizada¸ por lo que no desaparece la relación entre la finalidad perseguida que legitimó el tratamiento y el empleo de los datos. Por

todo ello, la cancelación (que se traduce en su supresión) de datos de salud debe tener un carácter excepcional.

Además, el titular de los datos podrá solicitar la suspensión del tratamiento, como medida cautelar de protección de sus datos mientras se impugna su exactitud y necesite los datos para reclamar, y cuando el tratamiento sea ilícito y se oponga a su supresión.

Del mismo modo, el titular de los datos tiene derecho, configurado en forma de prohibición al responsable del tratamiento, a que éste no adopte una decisión que se base únicamente en el tratamiento automatizado de sus datos o en la elaboración de perfiles que le pueda afectar significativamente; quedando excepcionado en los supuestos previstos en el apartado 2 del art. 22 RGPD, los cuales, sin embargo, quedarán inaplicados si se tratara de datos de salud y, por tanto, de datos de especial protección; salvo en el supuesto de que el titular de los datos haya dado su consentimiento explícito, o bien que el tratamiento sea necesario por razones de interés público esencial basado en el derecho nacional o de la UE.

OCTAVA. TRANSPARENCIA SANITARIA

Siguiendo con la determinación de la existencia de datos de salud dirigido a examinar como se realiza la protección de los mismos, llegamos a la transparencia pública, como principio legitimador democrático que garantiza una mayor participación de los ciudadanos en los asuntos públicos e instrumento de control de la actuación pública; manifestada mediante la transparencia pasiva o derecho de información o acceso, resultante del ejercicio del derecho de acceso ciudadano previsto en el art. 105.c) CE., y la transparencia o publicidad activa, derivada de la publicación obligatoria por las AAPP de la información (relacionada en los arts.6 a 8 LTBG) en el Portal de Transparencia, Portal Sanitario, como fuente de información en materia de sanidad o salud, que habrá de ser actualizada y sistematizada para su mejor uso; estando limitada si contiene datos personales y, en especial, datos de salud (o de especial protección), que únicamente podrán publicarse si son disociados, aplicándose los mismos límites (arts.14 y 15 LTBG) que a la publicidad pasiva.

En el ámbito sanitario, la transparencia juega un papel esencial, en la medida en que los datos de contenido sanitario permiten, por parte de las administraciones, planificar y evaluar el funcionamiento del Sistema sanitario y rendir cuentas sobre su gestión, mediante la necesaria publicidad de los elementos básicos de la actuación pública; lo que propicia lo posibilidad de ejercer responsabilidades. Del mismo modo, el acceso a los datos de salud constituye un elemento esencial en la mejora del sistema sanitario, por cuanto la información resultante del acceso por los ciudadanos permite que puedan actuar activamente mejorando la eficiencia del sistema.

NOVENA. REUTILIZACIÓN DE DATOS DE SALUD

En un escalón superior a la transparencia, la imparable evolución tecnológica ha afectado -aunque con retraso- al ámbito de la materia pública mediante la introducción de nuevos planteamientos en la forma del ejercicio de la función de gobernar derivados de la nueva figura del Gobierno Abierto (*Open Governement*), cuyos principios son la transparencia y el fomentar la participación y colaboración de ciudadanos y de las empresas; en este caso mediante la utilización de información (datos abiertos) accesibles, a través de un formato libre y legible mecánicamente en poder de los distintos organismos del sector público, excluyendo de ello los documentos previstos en el art. 3.3. de la Ley 37/2007, entre los que están los declarados limitados en su acceso o los que son incompatibles por tratarse de datos personales, como es el caso de la prevalencia de la protección de estos datos después de aplicada la ponderación prevista en los arts.3 y 15 LTGB, aunque puede permitirse su acceso si se disocian los datos.

Tratándose de la reutilización como una faceta del acceso a la información pública, los datos personales, al igual que para el acceso, constituyen un límite a su reutilización, al tratarse de un tratamiento de datos (cesión) que debe acomodarse al principio de calidad de datos, en cuanto a la adecuación y pertinencia de los datos (conforme a las condiciones destinadas a facilitar la reutilización previstas en la Directiva 2003/98/CE); requiriéndose para su cesión el consentimiento del interesado o que se cumplan las condiciones excepcionales previstas en el art. 6 RGPD; por lo que, a falta de ello, debe procederse a la disociación de la información a reutilizar, suprimiendo así la existencia de datos personales, como sería el caso de la información estadística, epidemiológica y de

investigación. La información, una vez reutilizada constituye, un fichero de datos, siendo el adquirente (cesionario) el responsable del cumplimento de las obligaciones previstas en la normativa sobre protección de datos.

DÉCIMA. INFORMACIÓN COMPRENSIVA DE DATOS DE SALUD

Junto a esta información de carácter general en el ámbito sanitario o de salud, que puede contener datos personales, podemos encontrarnos con otra información (en este caso directamente) comprensiva de datos de salud, como es la información asistencial o clínica, que comprende el derecho del paciente a conocer cualquier actuación relacionada con su estado de salud, sin perjuicio de no recibirla si el paciente así lo solicita o se estima en base a un estado de necesidad terapéutica; encontrándose condicionada, al tratarse de una información de carácter reservado que obliga a su confidencialidad por los profesionales tanto sanitarios como no sanitarios y su carácter previo a la emisión del consentimiento (informado) que, con carácter general, ampara el acceso a los datos sanitarios; y la derivada de la cesión de datos, incluidos los de carácter personal, que son necesarios para el funcionamiento del Sistema de información sanitaria.

Otra información comprensible de datos personales sería la relativa a investigación biomédica, contenida en la Ley de Investigación Biomédica, que deben recibir, de forma completa y comprensible, quienes participan en un proyecto de investigación si la misma tiene relevancia para su salud; y que, entre otros aspectos, incluirá las medidas que aseguren el respeto a la privacidad de los datos de acuerdo con la normativa sobre protección de datos. Por último, la información o publicidad sobre las listas de espera (quizás la que más problemas proporciona al SNS) supone una herramienta básica de medir la calidad de los servicios sanitarios; a pesar de que, en general, puede accederse a la información general y a tiempos medios de espera, únicamente el paciente afectado puede acceder a los datos asistenciales específicos de su proceso asistencial mediante su DNI inicial y clave posterior que proporciona el sistema informático.

UNDÉCIMA. DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA COMPRENSIVA DE DATOS DE SALUD

Además de la reutilización de la información pública, otro de los pilares en los que se apoya el *Open Governement* es el derecho de acceso a la información pública, calificado como derecho fundamental por la CDFUE (derecho fundamental autónomo e independiente de todos los ciudadanos europeos), por la jurisprudencia del TEDH y algún autor minoritario; lo que contrasta con la tendencia mayoritaria de considerarlo como derecho de configuración legal y no fundamental, siendo una manifestación del principio de transparencia; al mismo tiempo que constituye un derecho instrumental respecto de otros derechos, relacionado con la libertad de expresión y la libertad de información, reconocida ésta como "derecho a informarse" a través de fuentes públicas informativas, que después puedan permitir al ciudadano participar en la vida pública mediante sus opiniones o críticas, como derecho de participación, que también fundamenta el derecho de acceso.

La nueva LPAC ha extendido el derecho de acceso de todos los ciudadanos, más allá de lo que lo hacía la LTBG, a los archivos y registros y a la información pública, a través de todo contenido o documento que esté en poder de poder de los sujetos públicos relacionados en el art. 2 LTBG, ya que todos los documentos públicos lo son en general salvo que no pueda accederse para proteger otros derechos e intereses legítimos.

En el ámbito sanitario o de la salud, por tanto, sería susceptible de acceso toda la información de este tipo, tratándose una información amplia y variada, sometida en todo caso a la normativa sobre protección de datos: como, básicamente, la derivada de la cartera de prestaciones o servicios del SNS, dirigida a los pacientes como usuarios del Sistema sanitario y al mismo tiempo como herramienta de funcionamiento del propio sistema, constituyendo el Sistema de información sanitaria (previsto en la Ley de Cohesión) como instrumento esencial del SNS; la información epidemiológica y de salud pública, por la que los ciudadanos, salvo las limitaciones legales, tendrán derecho a ser informados de forma veraz y conforme a lo dispuesto en esta ley sobre los contenidos previstos en el art. 10 de la Ley General de Salud Pública, existiendo un Sistema de información en Salud Pública que incluirá toda la información necesaria (sobre todo estadística) que sirva de apoyo para la toma de decisiones en esta materia; y la información a pacientes y usuarios mediante el prospecto, la ficha técnica y el etiquetado

incluido en los medicamentos (de acuerdo con la Ley de garantías y uso racional del medicamento y productos sanitarios).

A propósito de la transparencia y accesibilidad de la información sanitaria y, en concreto, en materia de salud pública, en los momentos de redactar estas conclusiones, con ocasión de la pandemia del Covid-19, se está produciendo la problemática derivada de la opacidad del Gobierno en facilitar los nombres del Comité de Expertos en el coronavirus, que no facilita, entendiendo que se trata de asesores que no forman parte de la organización gubernamental.

Sin embargo, hay que señalar que esta actitud vulnera directamente: tanto la Ley de Salud Pública, que obliga a la transparencia en la información sobre salud pública; como la propia Ley de Transparencia, que determina que debe proporcionarse aquella información que sea de interés público, necesaria para el conocimiento de la población del control del funcionamiento de la actuación pública; en este caso, de las medidas adoptadas en esta epidemia.

DUODÉCIMA. PROCEDIMIENTO DE ACCESO A INFORMACIÓN PÚBLICA QUE CONTIENE DATOS DE SALUD

Conforme al procedimiento general, derivado de lo establecido en la LPAC, el acceso a la información pública se realizará, sin necesidad de motivación, previa solicitud dirigida al órgano administrativo que posea la información; el cual, después del análisis de los requisitos formales, examinará si concurre alguna de las causas de denegación, previstas en el art. 18.1TBG, que deben interpretarse restrictivamente, y cuya finalidad es evitar que se deniegue información importante para la rendición de cuentas, o el conocimiento de la toma de decisiones públicas y su aplicación.

Estos motivos de denegación se refieren a información: en curso de elaboración (por tanto, documentos no definitivos) o publicación general; que tenga carácter auxiliar o de apoyo y, por tanto, no se base en documentos sin terminar, siendo lo determinante su finalidad instrumental y no la denominación; aquella que para su divulgación necesita una tarea (compleja) de reelaboración previa, sin que el volumen sea decisivo, sino que se trate, de forma justificada, de un trabajo difícil y complejo a realizar que pueda poner

en peligro el normal funcionamiento del servicio público; aquella no disponible por el órgano, desconociendo quien la posee, que obliga a una nueva solicitud dirigida a otro órgano; y aquellas que, de forma justificada, se consideren manifiestamente repetitivas o abusivas que no se justifiquen con la finalidad de la ley, cual es el control de las decisiones y el manejo de fondos públicos, así como los criterios de actuación administrativa.

Posteriormente, el sujeto público procederá a examinar si el contenido de la información solicitada incluye datos de carácter personal (por tanto, que permita identificar a una persona física y hayan sido objeto de tratamiento), que suponen un límite excepcional al derecho de acceso; determinándose que, no cabe la exclusión absoluta de un derecho sobre el otro y de que la sola aparición de datos personales no supone que en principio deba denegarse el acceso por afectar a la intimidad o integridad personal.

Por tanto, la interacción del derecho a la protección de datos con el derecho de acceso se sustenta esencialmente en el art. 15 LTBG, que establece un conjunto de reglas para los distintos supuestos de acceso que se planteen, que deberán complementarse con las instrucciones y resoluciones de la AEPD y de las agencias autonómicas. Estas reglas se estructuran a partir de distintos niveles de protección y accesibilidad (mediante exenciones o limitaciones) en función del tipo de dato concreto que se pretende comunicar. En el caso de que la información contenga datos que puedan afectar a derechos e intereses de su titular o de otras personas deberá realizarse el trámite de audiencia a fin de que estas presenten alegaciones.

Así, en el supuesto de que se contengan datos de salud (de especial protección), habrá de considerarse la influencia de la normativa sanitaria con la de protección de datos y la finalidad de los datos de salud que es la atención sanitaria del paciente, que habrá de ser prevalente en todo caso; necesitándose, por tanto, una conciliación de los intereses en juego, mediante una interpretación amplia de las normas no sanitarias. En estos datos, sólo podrá comunicarse su acceso con el consentimiento del afectado (mediante un trámite de audiencia), si lo autoriza una ley, o que se hayan publicado por su titular (en cuyo caso, sí sería necesaria la ponderación de intereses al no existir consentimiento del titular).

Tratándose de datos públicos propios de empleados públicos meramente identificativos de los responsables de órganos y unidades administrativas (relacionados, por tanto, con

la organización en la que trabajan) y que se relacionan con el funcionamiento o actividad pública del órgano, prevalece el interés público de la información, excepto si aplicado al caso concreto existen prioritarios derechos constitucionalmente protegidos.

Por último, en el caso (residual respecto de los tipos de datos anteriores) de los datos personales de terceras personas (meramente identificativos y no especialmente protegidos) que sirven para identificar a una persona (sólo nombre y apellidos, salvo que se incluyan en una fuente de acceso público), el acceso deberá concederse con carácter general y sin necesidad de consentimiento, en la medida que implica un perjuicio menor para los derechos de los afectados.

Tratándose de datos que no sean de especial protección podrá disociarse la información si es de interés del solicitante.

DECIMOTERCERA. LIMITACIONES AL DERECHO DE ACCESO A INFORMACIÓN PÚBLICA COMPRENSIVA DE DATOS DE SALUD

El órgano administrativo, una vez comprobado la existencia de las excepciones legales que limitan el acceso como medidas preventivas de la protección de datos (y que funcionan como auténticas causas de denegación), debe proceder a su evaluación y valoración para determinar si se deniega o no la solicitud, o su acceso parcial. Así, mientras los límites previstos en el art. 14 LTBG (coincidentes con bienes constitucionalmente protegidos) tienen una aplicación directa; los límites contenidos en el art. 15, que no se aplican a los datos de salud, contienen una regla general favorable a la accesibilidad para los datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano; considerándose que no resultan aplicables si se impide la identificación del afectado mediante la disociación, y que su aplicación es facultativa para el sujeto público.

Para ello, el sujeto público deberá valorar restrictivamente estas limitaciones, de forma que tengan el mínimo alcance necesario, y de acuerdo con los principios de proporcionalidad y de finalidad de los datos, sin que pueda comunicarse una información que permita identificar a una persona, vulnerando el derecho a la protección de datos; en

cuyo caso podrá plantearse la concesión de un acceso parcial, que concilie los intereses enfrentados.

Por tanto, se realizará una primera evaluación ("test de daño") para determinar previamente los perjuicios concretos (se exige un daño real, efectivo y evaluable) que hipotéticamente pudieran provocar la comunicación de la información en el interés derivado de la necesaria protección de la privacidad, sin que puedan afectar a un determinado ámbito material, lo que excluiría el bloque completo de información; y, posteriormente se llevará a cabo una ponderación de intereses ("test de interés público"), a fin de definir, para el caso concreto de que se trate y mediante una aplicación proporcionada y limitada por su objeto y finalidad, si existe un interés público superior que justifique el acceso o comunicación de la información, asociado con la existencia de un interés racional y legítimo digno de protección; concretado, además de las excepciones en materia de seguridad nacional, defensa o relaciones exteriores (previstas en la LTBG), en distintos criterios interpretativos, como el acuñado por la AEPD: "(…) en cuanto el acceso a la información contribuya a un mejor conocimiento de los criterios de organización y funcionamiento de las instituciones o a la asignación de recursos, cabrá considerar la existencia de un interés público prevalente sobre los derechos a la protección de datos y a la intimidad en los términos y con las excepciones establecidas por la LTBG.

Al margen del interés público, otros criterios interpretativos que habrán de considerarse serían los propios de la protección de datos, así como los previstos en el apartado 3º del art. 15: como la posibilidad de denegar de forma motivada el acceso si la información contiene datos que puedan identificar a una persona, debiendo prevalecer la protección de la intimidad o de los menores (en su caso) sobre el acceso.

Otros criterios interpretativos serían: la mayor relevancia pública del titular de los datos, de los que se solicita la información; la satisfacción de un interés legítimo (lo que eximiría del consentimiento del afectado), como sería el facilitar los datos de terceros implicados en un proceso de selección pública; o la consideración de que, en la medida en que la información afecte directamente a la organización o actividad pública del órgano, prevalecerá el acceso. Además, procede aplicar la LTBG si se trata de datos personales de terceros, mientras si son datos del solicitante se aplica la normativa sobre protección de datos, la cual limita el acceso ante la necesaria protección de los derechos e intereses de terceros afectados, como la protección de la intimidad en el acceso a las anotaciones

subjetivas en la HC. En el caso de que la información solicitada contuviera al mismo tiempo datos personales del solicitante y datos de terceros procedería aplicar la LTBG, por cuanto el derecho de acceso no alcanza a los datos personales de un tercero.

DECIMOCUARTA. ESPECIFICIDADES DE LOS DATOS DE SALUD

A lo largo de todo este trabajo hemos podido ver la evolución del derecho a la protección de datos y su vinculación con la intimidad (o privacidad, en términos más amplios): desde su reconocimiento inicial en instrumentos jurídicos internacionales y europeos y en la normativa y jurisprudencia de la UE (en los que ya se contempla la protección especial que debe dispensarse a los datos de salud), sin olvidar la trascendental Sentencia sobre el Censo del TC Alemán (reconocedora de la autodeterminación informativa del individuo sobre sus datos), a la práctica jurisprudencial constitucional nacional; para pasar después a su reconocimiento normativo, modificado posteriormente por la LOPD y, recientemente actualizados a través del RGPD y la LOPDGDD.

Así, a lo largo de este trabajo hemos podido comprobar como la nueva normativa sobre protección de datos y los nuevos principios que incorpora, inciden de forma directa y sustancial en la protección de la privacidad en la materia sanitaria o de salud de una forma positiva y efectiva; de forma que, partiendo de la mayor trascendencia atribuible a este tipo de datos, han venido a reforzar aún más la protección dispensada por la anterior normativa. Así, se ha reforzado la protección en el tratamiento de los datos de salud, estableciendo, con carácter general, su prohibición, al margen del consentimiento de su titular, y de las habilitaciones legales previstas en base al interés público, con las garantías de protección adecuadas.

Además, la nueva concepción de seguridad de los datos, basada en la adopción previa de medidas proactivas y preventivas adaptadas al riesgo de máximo nivel de daño previsto para los datos sanitarios, con la necesaria Evaluación de impacto previa al tratamiento de datos, suponen una garantía añadida muy importante para la protección de los datos de salud. Dentro del ámbito de la seguridad, este reforzamiento se aprecia, igualmente, al examinar las medidas de protección de la intimidad y de la confidencialidad a las que deben someterse el *Big Data* y las nuevas TICs sanitarias, y demás soluciones tecnológicas de *eHealth*. No olvidemos, además, de la garantía que supone el que los

datos de salud están excluidos de la aplicación obligatoria del test de daño y el del test de intereses, tratándose de solicitudes de información pública.

Por todo ello, podemos concluir que, después de examinado todo el ámbito de afectación de la materia sanitaria y de salud pública al conjunto del sistema sobre protección de datos personales (normativa, jurisprudencia, doctrina científica, resoluciones de autoridades de control y consejos de transparencia): la actual regulación sobre protección de datos, necesariamente conciliada con la propiamente sanitaria o de salud, en una interpretación conjunta amplia y flexible, adaptada a la finalidad asistencial, en comparación con la anterior normativa sobre la materia (de necesaria invocación interpretativa a falta de regulación aplicable al caso concreto), ha añadido un plus de protección; garantizando de forma adecuada y suficiente la protección de los datos de salud, adaptada a la nueva realidad tecnológica que estamos viviendo vertiginosamente. Ello, sin perjuicio, de la posibilidad (y necesidad) de adopción o de adecuación de medidas complementarias de protección de la privacidad sanitaria, amparadas por la normativa conjunta de protección de datos y de regulación de la asistencia sanitaria y salud pública.

Además, Los datos sanitarios o de salud, por su esencial finalidad de servir de instrumento de curación y protección o mejora de la salud, constituyen un tipo especial de datos personales, con un contenido específico y claramente diferenciado del resto de datos personales, que, por todo ello, les hace necesariamente merecedores de la más alta protección jurídica. Y, esta protección, se manifiesta no sólo básicamente en el principio general de la prohibición de su tratamiento, excepto si concurre el consentimiento del afectado y existe habilitación legal suficiente, sino respetando (dada su esencial finalidad) sus especificidades en relación con los demás datos de carácter general, e incluso de los datos de su propia categoría (especialmente protegidos). De ahí, que las distintas particularidades de los datos de salud que hemos visto a lo largo de este trabajo (como en los ámbitos del consentimiento, acceso y conservación de la HC, cancelación, etc.), amparadas por la aplicación a los casos concretos de la normativa específica sanitaria (LBAP, Ley de Cohesión y Calidad del Sistema Nacional de Salud…) han venido a conceder a los titulares de datos de salud derechos diferenciados respecto de los demás datos de carácter personal; en la medida en que, como legislación especial, debería aplicarse preferentemente la normativa sanitaria. No obstante, este postulado no debería llevarse a su aplicación estricta, en la medida en que los principios y normas del RGPD

son de aplicación directa; por ello, se impone una adecuada conciliación y una interpretación amplia, coordinada y equilibrada entre la normativa general sobre protección de datos (RGPD y LOPDGDD) y la específica normativa sanitaria, en beneficio (en todo caso) de la mejora de la asistencia sanitaria del paciente.

JURISPRUDENCIA

I. TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (TJUE)

STJCE de 12 de noviembre de 1969, asunto *Stauder v. Stadt Ulm-Sozialamt*

STJUE 178 de 9 de septiembre de 1999, asunto *Andrea Krüger v. Kreiskrankenhaus Ebersberg*

STJUE de 20 de mayo de 2003, asunto *Rundfunk* y otros

STJCE de 6 de noviembre de 2003, asunto *Sra. Lindqvist*

STJUE de 8 de noviembre de 2007, *Bavarian Lager contra Comisión*

STJUE de 9 de marzo de 2010: asunto *Comisión v. Alemania*

STJUE de 29 de junio de 2010, asunto *Comisión Europea contra The Bavarian Lager Co. Ltd.* Esta sentencia anula la STJUE de 8 de noviembre de 2007, asunto *Bavarian Lager contra Comisión*

STJUE de 15 de julio de 2010, asunto *Bianca Purrucker contra Guillermo Vallés Pérez*

STJUE de 9 de noviembre de 2010, asunto *Volker und Markus y Hartmut Eifert*

STJUE de 22 de marzo de 2011, asunto *Access Info Europe contra Consejo*

STJUE de 24 de noviembre de 2011, asunto *Comisión contra España*

STJUE de 16 de octubre de 2012, asunto *Comisión v. Austria*

STJUE C-486/12, de 12 de diciembre de 2013, asunto *Proceedings brought by X*

STJUE de 17 de octubre de 2013, asunto *Consejo contra Access Info Europe*

STJUE de 12 de diciembre de 2013, asunto *Carmela Carratù contra Poste Italiane SpA*

STJUE de 8 de abril de 2014, asunto *Comisión v. Hungría*

STJUE de 13 de mayo de 2014, asunto *Google Spain SL c/Agencia Española de Protección de Datos*

II. OTROS TRIBUNALES INTERNACIONALES

STPI asunto T-2/03, *Verein für Konsumenteninformation v. Comisión*

STEDH de 12 de julio de 1977, caso *Brüggeman and* Scheuten

STEDH de 6 de septiembre de 1978, caso *Klass y otros*

STEDH de 22 de octubre de 1981, caso *Dudgeon*

STEDH de 26 de marzo de 1987, caso *Leander*

STEDH 26 de octubre de 1988, caso *Norris*

STEDH de 7 de julio de 1989, caso *Gaskin*

STEDH de 26 de noviembre de 1991, caso *Chassagnou*

STEDH de 16 de diciembre de 1992, caso *Niemietz*

STEDH de 22 de febrero de 1994, caso *Burghartz*

STEDH de 25 de noviembre de 1994, caso *Stjerna*

STEDH de 19 de febrero de 1997, caso *Laskey Jaggard*

STEDH de 24 de febrero de 1998, caso *Botta*

STEDH de 16 de febrero de 2000, caso *Amann*

STEDH de 4 de mayo de 2000, caso *Rotaru*

STEDH de 16 de abril de 2002, caso *Stés Colas Est*

STEDH de 22 de octubre de 2002, caso *Taylor-Sabori*

STEDH de febrero de 2003, caso *Odiévre*

STEDH de 24 de julio de 2003, caso *Smirnova*

STEDH de 27 de abril de 2004, caso *Doerga*

STEDH de 31 de mayo de 2005, caso *Vetter*

STEDH de 19 de abril de 2009, caso *Társaság a Szabadságjogokért v. Hungary*

STEDH de 25 de junio de 2013, caso *Youth Initiative for Human rights v. Serbia*

STEDH de 8 de noviembre de 2016, caso *Magyar Helsinki Bizottság c. Hungría*,

III. TRIBUNAL CONSTITUCIONAL (TC)

STC 11/1981 de 8 de abril

STC 2/1982 de 29 de enero

STC 73/1982, de 2 de diciembre

STC 110/1984, de 26 de noviembre

STC 107/1987, de 25 de junio,

STC 20/1988, de 18 de febrero

STC 231/1988, de 2 de diciembre

STC 197/1991, de 17 de octubre

STC 220/1991 de 25 de noviembre

STC 142/1993, de 22 de abril

STC 254/1993, de 20 de julio

STC 57/1994, de 28 de febrero

STC 143/1994, de 9 de mayo

STC 117/1994, de 25 de abril

STC 102/1995, de 26 de junio

STC 119/1995, de 17 de julio

STC 34/1996, de 11 de marzo

STC 15/1997, de 30 de enero

STC 94/1998, de 4 de mayo

STC 18/1999, de 22 de febrero

STC 134/1999, de 15 de julio

STC 144/1999, de 22 de julio

STC 202/1999, de 8 de noviembre

STC 290/2000, de 30 de noviembre

STC 156/2001 de 2 de julio

STC 99/2002, de 6 de mayo

STC 121/2002, de 20 de mayo

STC 292/2002, de 30 de noviembre

STC 196/2004, de 15 de noviembre

STC 62/2007 de 27 de marzo

STC 159/2009 de 29 de junio

STC 37/2011, de 28 de marzo

STC 17/2013, de 31 de enero

STC 545/2015, de 15 de octubre

STC 39/2016, de 3 de marzo

STC 76/2019, de 22 de mayo

IV. TRIBUNAL SUPREMO (TS)

STS de 6 de octubre de 1979

STS de 7 de marzo de 1985

STS de 9 de julio de 1986

STS de 15 de enero de 1987

STS de 4 de julio de 1987

STS de 22 de octubre de 1987

STS de 9 de junio de 1988

STS de 14 de diciembre de 1988

STS de 16 de diciembre de 1988

STS de 1 de julio de 1991

STS de 31 de mayo de 1995

STS de 30 de marzo de 1999

STS de 25 de octubre de 1999

STS de 14 de noviembre de 2000

STS de 12 de febrero de 2002

STS de 20 de octubre de 2003

STS de 1 de febrero de 2006

STS de 30 de mayo de 2007

STS de 30 de diciembre de 2009

STS de 30 de diciembre de 2009

STS de 14 de febrero de 2012

STS de 24 de octubre de 2013.

STS de 15 de octubre de 2015

STS de 21 de diciembre de 2015

STS de 16 de octubre de 2017

STS de 16 de octubre de 2017

STS de 5 de febrero de 2019

V. AUDIENCIA NACIONAL (AN)

SAN de 8 de marzo de 2002

SAN 26 de noviembre de 2003

SAN de 24 de marzo de 2006

SAN de 8 de febrero de 2006

SAN de 17 de abril de 2007

SAN de 9 mayo de 2007

SAN de 8 de octubre de 2008

SAN de 8 de abril de 2010

SAN de 30 de junio de 2011

SAN de 6 de noviembre de 2013

SAN de 26 de noviembre de 2013

SAN de 3 de marzo de 2014

SAN de 19 de marzo de 2014

SAN de 31 de marzo de 2015

SAN de 15 de julio de 2016

SAN de 28 de octubre de 2016

SAN de 18 de septiembre de 2019

VI. TRIBUNAL SUPERIOR DE JUSTICIA (TSJ)

STSJ Madrid, Sala de lo Contencioso Administrativo, de 28 de febrero de 2006

STSJ Cataluña, Sala de lo Contencioso-Administrativo, de 5 de octubre de 2010

VII. AUDIENCIA PROVINCIAL (AP)

SAP de Sevilla, de 20 de junio de 2006

SAP de Barcelona, de 11 de octubre de 2013

SAP de Navarra, de 7 de diciembre de 2016

SAP de Navarra, de 3 de abril de 2017

VIII. JUZGADOS DE LO CONTENCIOSO-ADMINISTRATIVO

Sentencia del Juzgado Central de lo Contencioso-Administrativo nº 9, de 25 de abril de 2016

Sentencia del Juzgado Central de lo Contencioso-Administrativo n° 5 de Madrid, de 14 de junio de 2016

Sentencia del Juzgado Central de lo Contencioso-Administrativo nº 11 de Madrid, de 22 de marzo de 2017

Sentencia del Juzgado Central de lo Contencioso-Administrativo n° 11 de Madrid, de 22 de junio de 2017

Sentencia del Juzgado Central de lo Contencioso- Administrativo n° 7 de Madrid, de 3 de abril de 2018

AUTORIDADES DE CONTROL

I. AUTORIDADES DE PROTECCION DE DATOS

A) AUTORIDAD NACIONAL (AEPD)

A1. *Criterios interpretativos*

- CI/002/2015, de 24 de junio de 2015.
- CI/004/2015, de 23 de julio de 2015.
- CI/007/2015, de 12 de noviembre de 2015.
- CI/008/2015, de 12 de noviembre de 2015.
- CI/009/2015, de 12 de noviembre de 2015.
- CI/009/2015, de 12 de noviembre de 2015.
- CI/002/2016, del 05 de julio de 2016.

A2. *Resoluciones*

- Resolución de 22 de noviembre de 2004.
- Resolución de 31 de mayo de 2005.
- Resolución de 30 de marzo de 2007.
- Resolución de 8 de septiembre de 2009.
- Resolución R/01461/2010.
- Resolución R/01627/2012.
- Resolución de 19 de septiembre de 2013.
- Resolución RE 241/2015, de 21 de octubre de 2015.
- Resolución R/032/2016, de 27 de octubre de 2016.

- Resolución R/65/2016, de 23 de mayo de 2016.
- Resolución R/151/2016, de 17 de mayo de 2016.
- Resolución R/0290/216, de 30 de septiembre de 2016.
- Resolución R/393/2016, de 21 de noviembre de 2016.
- Resolución R/0432/2016, de 22 de diciembre de 2016.
- Resolución R/0433/2015, de 15 de febrero de 2016.
- Resolución R/132/2017, de 7 de agosto de 2017.
- Resolución R/406/2017, de 23 de noviembre de 2017.
- Resolución RT/0376/2018, de 4 de febrero de 2018.
- Resolución de 15 de enero de 2019.
- Resolución R/103/2019 del CTBG de 8 de mayo de 2019.
- Resolución RT nº 171/2019, de 29 de mayo de 2019.

A3. ***Informes***

- Informe 0445/2009.
- Informe de 5 de junio de 2007.
- Informe 0341/2009.
- Informe 036/2004.
- Informe 0437/2012.
- Informe 0049/2007
- Informe 0017/2020
- Informe 0452/2012.
- Informe de 28 de mayo de 2010.
- Informe 0248/2005.
- Informe septiembre de 2018
- Informe 0194/2010.

A4. *Procedimiento de Tutela de derechos*

- Resolución Procedimiento de Tutela de derechos TD/00884/2013.

B) SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

- Dictamen 3/2015, de 28 de julio.

C) AEPD. OTROS DOCUMENTOS

- Memoria de la AEPD de 2014, publicada con fecha de 30 de junio de 2015.

II. CONSEJOS DE TRANSPARENCIA

A. CONSEJO DE TRANSPARENCIA Y BUEN GOBIERNO (CTBG)

- Resolución nº 52-RT/2017 de 9 de mayo.
- Resolución nº 284-RT/2016, de 16 de marzo de 2017.
- Resolución nº 197/2018, de 29 de junio de 2018.

B. CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA (CTPD)

- Resolución RE/241/2018, de 13 de junio de 2018.
- Resolución RES/042/2016, de 22 de junio.
- Resolución RE/132/2016, de 21 de diciembre de 2016.
- Resolución RES/002/2017, de 4 de enero de 2017.
- Resolución RES/042/2016, de 22 de junio de 2016.
- Resolución 106/2016, de 16 de noviembre.

- Resolución RES/85/2019, de 1 de abril de 2019.
- Resolución RES/32/2016, de 1 de julio de 2016.
- Resolución RE/64/2016, de 20 de julio.
- Resolución RE/181/2018, de 23 de mayo de 2018.
- Resolución RES/34/2019, de 18 de febrero de 2019.
- Resolución RES/042/2016, de 22 de junio de 2016.
- Resolución RES/197/2018, de 29 de junio.
- Resolución RE/38/2019, de 19 de febrero de 2019.
- Resolución RES/042/2016, de 22 de junio de 2016.
- Informe nº 145/2016, de 15 de noviembre.

C. OTROS

- Criterio del Consejo de Europa en el Convenio sobre Acceso a los Documentos Públicos.
- Informe conjunto del CTBG y de la AEPD, de 23 de marzo de 2015.
- Criterio interpretativo conjunto del CTBG y AEPD, CI/001/2015, de 23 de marzo de 2015.

GT ART. 29 DIRECTIVA 45/96/CE

- Dictamen 5/2001, relativo el Informe Especial del Defensor del Pueblo Europeo al Parlamento Europeo sobre el proyecto de Recomendación dirigido a la Comisión Europea en la reclamación 713/98/IJH, de 17 de mayo de 2001.

- Documento de 17 de marzo de 2004, sobre datos genéticos.

- Documento de trabajo 00323/07/ES WP 131, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), adoptado el 15 de febrero de 2007.

- Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007.

- Dictamen 3/2010, W 173, de 13 de julio de 2010, sobre el principio de responsabilidad activa ("*accountability*").

- Dictamen 15/2011, adoptado el 13 de julio de 2011 (WP 187) sobre la definición de consentimiento (WP 187), y el Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos.

- Artículo "*Health data in apps and devices"*, de 9 de febrero de 2015.

- Guía W 248, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679, W 248, adoptada el 4 de abril de 2017.

- Directrices sobre la aplicación y fijación de multas administrativas a efectos del Reglamento 2016/679, adoptadas el 3 de octubre de 2017.

- Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, adoptadas el 3 de octubre de 2017.

- Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 28 de noviembre de 2017.

- Directrices del GT29 sobre el consentimiento en el sentido del RGPD, adoptadas el 28 de noviembre de 2017.

- Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, adoptadas el 29 de noviembre de 2017.

- Directrices sobre el derecho a la portabilidad de datos del Grupo de Autoridades europeas de Protección de Datos", adoptadas el 12 de enero de 2017.

BIBLIOGRAFÍA

ABELLÁN, F., y SÁNCHEZ CARO, J., "Telemedicina y protección de datos sanitarios (aspectos legales y éticos)", Comares, Granada, 2002.

ABERASTURI GORRIÑO, A., "La protección de datos en la sanidad", Aranzadi-Thompson, Pamplona 2013.

AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID, "Manual de protección de datos para las Administraciones Públicas", Civitas, Madrid, 2004.

"Protección de datos personales para servicios públicos sanitarios", Aranzadi-Thompson, Pamplona, 2008.

ALVÁREZ CARO, M., "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones…", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* PIÑAR MAÑAS, J.L. (Director), Reus Ediciones, Madrid, 2016.

"El derecho a la supresión o al olvido", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* PIÑAR MAÑAS, J.L. (Director), Reus Ediciones, Madrid, 2016.

"El derecho a la supresión o al olvido", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* PIÑAR MAÑAS, J.L. (Director), Reus Ediciones, Madrid, 2016.

ÁLVAREZ GONZÁLEZ, S., y GARRIGA DOMÍNGUEZ, A., "Historia clínica y protección de datos (especial referencia al registro obligatorio de los portadores de VIH)", Dykinson, Madrid, 2011.

ÁLVAREZ HERNANDO, J., "Tratamiento de datos personales en la Administración Pública", *Practicum Protección de Datos,* Aranzadi, Pamplona, 2014.

ANDREU MARTÍNEZ, M, "Open data en el ámbito sanitario y su compatibilidad con la privacidad del paciente", Accueil -Les Éditions de L,IMODEV, vol 5, 2017.

APARICIO SALOM, J., "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", 2ª ed., Aranzadi, Cizur Menor, Pamplona, 2002.

ARENAS RAMIRO, M., y otro, "Comentarios a la Ley Orgánica de protección de datos y garantía de Derechos Digitales (en relación con el RGPD)", Edit. Sepin, 2019.

"El Derecho Fundamental a la Protección de Datos Personales en Europa. Monografías", Tirant lo Blanch, Valencia, 2006.

"Reforzando el ejercicio del derecho a la protección de datos personales, hacia nuevo derecho europeo de protección de datos", Tirant Lo Blanch, Valencia, 2015.

"El Principio del Consentimiento en los Estados miembros de la Unión Europea",Tirant lo Blanch, Vol.2, Valencia, 2007.

ARRUEGO, G., "La naturaleza constitucional de la asistencia sanitaria no consentida y los denominados supuestos de "urgencia vital", *Revista Española de Derecho Constitucional*, nº 82, 2008.

ASOCIACIÓN ESPAÑOLA DE CIRUJANOS, "El consentimiento informado en cirugía", Editores Médicos, Madrid, 1998.

ATELA BILBAO, A., y otros, "Autonomía del paciente, información e Historia clínica. Estudios sobre la Ley 41/2002, de 14 de noviembre", GONZÁLES SALINAS y LIZARRAGA BONELLI (coords), Edit, Thomson-Civitas, Pamplona, 2004.

BARNÉS, J., "El principio de proporcionalidad. Estudio preliminar", *Cuadernos de Derecho Público*, n º 5, 1998.

BARRIO ANDRÉS, M., "Fundamentos del Derecho de Internet", *Centro de Estudios Políticos y Constitucionales*, Madrid, 2017.

BLANES CLIMENT, M.A., "La transparencia informativa de las Administraciones públicas. El derecho de las personas a saber y la obligación de difundir información pública de forma activa", Thomson-Reuters Aranzadi, Pamplona, 2014.

CAVOUKIAN, Ann, "*Privacy by Design, The 7 Foundational Principles*". Agosto 2009. Accessible en: www.ipc.on.ca.

CARNICERO GIMÉNEZ DE AZCÁRATE, J., "El derecho a la protección de datos en la historia clínica y la receta electrónica", Aranzadi, Pamplona, 1999.

CEA EGAÑA, J.L., *Revista de Derecho y Ciencias Penales*, Universidad de San Sebastián (Chile), 2009, pp.31-33.

CHUECA SANCHO, A.G., "La evolución de los derechos fundamentales en los tratados comunitarios", en MATIA PORTILLA, F.J., en *La protección de los derechos fundamentales en la Unión Europea,* Civitas, Madrid, 2002.

CÓDIGO DE DEONTOLOGÍA MÉDICA DE LA OMC, de julio de 2011.

COLLADO GARCÍA-LAJARA, E, "Protección de datos de carácter personal (legislación, comentarios, concordancias y jurisprudencia)", Comares, Granada 2000.

CONDE ORTIZ, C., "La protección de datos personales. Un derecho con base en los conceptos de intimidad y privacidad", Dykinson, Madrid, 2005.

CORRAL SASTRE, A., "Art 63-69, Procedimiento sancionador en materia de protección de datos". Comentarios a la nueva Ley de Protección de datos. Ley Órganica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantías de los Derechos Digitales. Coord por Alejandro Villanuevas Turnes, Ana Isabel Berrocal Lanzarot, (pr.) 2020.

" El régimen sancionador en materia de protección de datos en el Reglamento General de la UE", en "Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*",* PIÑAR MAÑAS, J.L. (Director), Reus Ediciones, Madrid, 2016.

"El acceso a la información ambiental en España a la luz de la nueva ley de transparencia." Acceso à informacâo como direito fundamental e dever estatal. Coord por Ingo Wolfgang Sarlet, Jose Antonio Montilla Martos, Regina Linden Ruaro 2016, pp. 205-229.

CRISTEA ULIVARU, L., "Protección de datos de carácter sensible: historia clínica digital y big data", Edit. Bosch, Barcelona, 2018.

DAVARA RODRÍGUEZ, M.A., "La protección de datos en Europa: principios, derechos y procedimientos", Universidad de Comillas, Madrid, 1998.

"Una primera aproximación al Reglamento europeo de protección de Datos y su incidencia en el tratamiento de datos de carácter personal de las Administraciones Públicas», *Actualidad Administrativa,* N° 4.

DEBBASCH, C., Introducción, en "La transparence administrative en Europe", Editions du Centre National de la Recherche Scientifique, Paris, 1990.

DEPARTAMENTO JURÍDICO DE SEPIN DERECHO SANITARIO, "Guía práctica de protección de datos en el ámbito sanitario. Comentarios doctrinales, normativa, Cuadros legislativos y comparativos, Esquemas y formularios", Sepin, Madrid, 2019.

DE LORENZO Y MONTERO, R., "Protección de datos personales en el sector sanitario", Edit. Colex, La Coruña, 2009.

"Derechos y obligaciones de los pacientes. Análisis de la Ley 41/2002, de 14 de noviembre, básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica", Edit. Colex, Madrid, 2003.

DE MIGUEL SÁNCHEZ, N., "Intimidad e historia clínica en la nueva la Ley 41/2002, de 14 de noviembre, básica reguladora de autonomía de los pacientes y de los

derechos de información y documentación clínica", *Revista española de Derecho administrativo*, nº 117, 2003.

DEL PESO NAVARRO, E., "*Ley de Protección de Datos: la nueva LORTAD"*, Díaz de Santos, Madrid, 2000.

DÍAZ-ROMERAL, GÓMEZ, A., "*Tratado de contratos del sector público*". Capítulo VII. Protección de datos y contratación pública. Coord. coord. por Isabel Gallego Córcoles, Eduardo Gamero Casado, Vol. 1, 2018 (Tomo I).

"Los códigos de conducta en el Reglamento de Protección de Datos", en "Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*",* PIÑAR MAÑAS, J.L. (Director), Reus Ediciones, Madrid, 2016.

"*La sede electrónica: eje vertebrador del derecho de los ciudadanos a la información, la participación y a relacionarse por medios electrónicos con las administraciones públicas*". Administración electrónica y ciudadanos / José Luis Piñar Mañas (dir.), 2011.

DÍEZ-PICAZO GIMÉNEZ, L.M., "Sistema de Derechos fundamentales*",* Thompson, Madrid, 2013.

DOMÍNGUEZ LUELMO, A., "Derecho sanitario y responsabilidad médica. Comentarios a la Ley 41/2002, de 14 de noviembre, básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica", Edit. Lex Nova, 2ª edic., Valladolid, 2007.

DOPAZO FRAGUIO, P., "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente", *Revista Española de Derecho Europeo* nº 68/2018, Civitas, Aranzadi, Pamplona, 2018;

"La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente", *Revista Española de Derecho Europeo* nº 68/2018, Civitas, Aranzadi, Pamplona, 2018.

DUASO CALÉS, R., "Los principios de protección de datos desde el diseño y protección de datos por defecto", en "Reglamento General de Protección de Datos. Hacia un

nuevo modelo europeo de privacidad*",* PIÑAR MAÑAS, J.L. (Director), Reus Ediciones, Madrid, 2016.

EL EMAM K, y ÁLVAREZ C. *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techiques*. In Data Privacy Law 2015.

ENÉRIZ OLAECHEA J, "Reglamento General de Datos personales y derecho de acceso a la información pública, o cómo conectar ambos", *Revista Aranzadi Doctrinal*, nº 9/2018, Editorial Aranzadi, 2018.

ESTUDIO "*Ubiquitous Developments of the Digital Single Market*" (Servicios de ubicuidad en el mercado único digital), elaborado por el Departamento Temático A y la agrupación de Wik-Consult, RAND Europe y TNO para la Comisión de Mercado Interior y Protección del Consumidor en 2013.

FARRÉ TOUS, S., "Principios de la protección de datos: acceso a los datos por cuenta de terceros. El encargado del tratamiento en el ámbito de las administraciones públicas", en *Comentario a la Ley de protección de datos, comentario al art.12 LOPD,* TRONCOSO REIGADA (coord..), Civitas, Madrid, 2010.

FERNÁNDEZ RAMOS, S., "El acceso a la información en el Proyecto de Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno", en "Transparencia, participación ciudadana y Administración pública en el siglo XXI", *Monografías de la Revista Aragonesa de Administración*, XIV, 2013.

"La Transferencia Pública: Pasado, Presente y Futuro". *Revista Aragonesa de Administración Pública*, núm. 51, Zaragoza, 2018.

"Acceso a la información pública versus protección de datos personales", *Revista Española de Derecho Administrativo* nº 184/2017, Civitas, Pamplona, 2017.

"Transparencia, Acceso a la Información Pública y Buen Gobierno, Ley 19/2013, de 9 de diciembre", Thomson Reuters, Pamplona, 2014.

FERNÁNDEZ RODRÍGUEZ, T.R., "La organización territorial del Estado y la Administración Pública en la nueva Constitución", en "*Lecturas sobre la Constitución Española"* (I), UNED, Madrid, 1978.

FERNÁNDEZ-RUIZ GÁLVEZ, E., "Intimidad y confidencialidad en la relación clínica", *Servicio de Publicaciones de la Universidad de Navarra,* Persona y Derecho, Vol. 69, Pamplona, 2013.

FERNÁNDEZ SALMERON, M., "La protección de los datos personales en las Administraciones Públicas", Civitas, Madrid, 2003.

FERNÁNDEZ SALMERÓN, M., y VALERO TORRES, J., "Transparencia administrativa y protección de datos personales. V encuentro de Agencias Autonómicas de protección de datos personales", Thomson-Civitas, Madrid, 2008.

GARCÍA MURCIA, J., RODRÍGUEZ CARDO, I.A., "Asistencia sanitaria transfronteriza en el ámbito de la unión europea: de la seguridad social de trabajadores migrantes a una regulación específica", *Foro Nueva Época,* vol.17, nº 1, 2014.

GARTNER: https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/#5a57875342f6

GARRIGA GONZÁLEZ, Ana, "El derecho a la autodeterminación informativa", en PÉREZ LUÑO, A., *Problemas actuales de documentación y la información jurídica,* Tecnos, Madrid, 1987.

GIL MEMBRADO, C., "La historia clínica. Deberes del responsable del tratamiento y derechos del paciente*"*, Cap.I, normativa, Comar, 2010.

GONZÁLEZ LÓPEZ, U., "El derecho a la portabilidad en el Reglamento General Europeo de Protección de Datos", LegalToday, http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-prodat/el-derecho-a-la-portabilidad-de-los-datos-en-el-reglamento-general-europeo-de-proteccion-de-datos

GONZÁLEZ MURÚA, A.R., "Comentario a la STC 254/1993, de 20 de julio. "Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales", *Revista Vasca de Administración Pública,* nº 37, 1993.

GRUPO EUROPEO DE ÉTICA DE LA CIENCIA Y DE LAS NUEVAS TECNOLOGÍAS, 30 de julio de 1999.

GUICHOT REINA, E., "Transparencia y protección de datos en las Universidades públicas", Revista española de Derecho Administrativo num.193/2018, parte Estudios, Editorial Civitas, Pamplona. 2018.

"Transparencia, Acceso a la Información Pública y Buen Gobierno", Tecnos, Madrid, 2014.

"Transparencia y Buen Gobierno, Código Básico" Universitario-Codex-Aranzadi, Edit.Aranzadi, 2014.

"Las relaciones entre transparencia y privacidad en el Derecho comunitario ante la reforma de la normativa sobre acceso a los documentos públicos", *Revista Española de Derecho Europeo* nº 37/2011, Civitas, Pamplona, 2011.

"Principios de la protección de datos: comunicación de datos por las administraciones públicas a sujetos privados", en *Comentario a la Ley Orgánica de Protección de datos de carácter personal*, TRONCOSO REIGADA, A., (Coord.), Civitas, Madrid, 2010.

"Publicidad y privacidad de la información administrativa", Thomson Reuters y AGPDCM, Madrid, 2008.

"Un paso decisivo en la clarificación de las relaciones entre derecho de acceso y derecho a la protección de datos: La Sentencia del TPI de 8 de noviembre de 2007, Bavarian Lage/Comisión, T.194/04", *Revista Española de Derecho europeo*, nº 27/2008, Civitas, Madrid, 2008.

"Acceso a la información en poder de la Administración y protección de datos personales", Revista de Administración Pública nº 173, 2007.

"Datos personales y Administración Pública", Thompson-Civitas, Madrid, 2005.

"El nuevo derecho de acceso a la información pública", en Revista de Administración Pública, nº 160, enero-abril, 2003.

GUTIÉRREZ GUTIÉRREZ, I., "Dignidad de la persona y derechos fundamentales", Marcial Pons, Madrid, 2005.

HERNÁNDEZ BEJARANO, M., "La Ordenación sanitaria en España", Edit, Thomson-Civitas, Pamplona, 2004.

HERNÁNDEZ CORCHETE, J.A., "Transparencia en la información al interesado del tratamiento de sus datos personales", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus Ediciones, 2016.

"El derecho de los ciudadanos a relacionarse con las administraciones publicas utilizando medios electrónicos y los derechos complementarios que delimitan su alcance" en Transparencia, Acceso a la Información y Protección de Datos dirigido por José Luis Piñar Mañas, REUS, Madrid, 2015.

HERRAN ORTIZ, A, "El derecho a la protección de datos personales en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos*, nº 26, Universidad de Deusto, Vizcaya, 2003.

"La violación de la intimidad en la protección de datos personales", Dickynson, Madrid, 1999.

IBERLEY INFORMACIÓN LEGAL. Disponible en https://www.iberley.es/temas/regimen-sancionador-materia-proteccion-datos-62809

JUNCEDA MORENO, J., "Obligaciones sobre transparencia. Protección de datos. Sobre los límites de la transparencia en el ámbito local", *La Administración Práctica*, nº 8/2016, Aranzadi, Pamplona, 2016.

LAZPITA GURTUBAN, M, "Análisis comparado de las legislaciones sobre protección de datos de los Estado miembros de la Comunidad Europea", Informática y Derecho, *Revista Iberoamericana de Informática y Derecho*, 1994.

LEGALIA, compañía de Servicios Jurídicos, "La protección de datos personales en el ámbito sanitario" Aranzadi-Thompson, Pamplona, 2002.

LIZARRAGA BONELL, E., "La información y la obtención del consentimiento", en *La nueva Ley 41/2002, Básica Reguladora de la Autonomía del paciente, en Autonomía del Paciente e información clínic*a, Thomson-Civitas, Madrid, 2004.

LÓPEZ GARCÍA, M., "Derecho a la información y derecho al olvido en Internet", *La Ley Unión Europea*, nº 17, julio 2014.

LÓPEZ ULLA, J.M., "Principios de la protección de datos: datos especialmente protegidos, en *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*, TRONCOSO REIGADA, A., (Coord.), Aranzadi, Pamplona, 2010.

MARTÍNEZ GUTIÉRREZ, R., "Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información", y VALERO TORRIJOS, J. Fernández Salmerón (coords.), Thompson Reuters, Pamplona, 2004.

MARTÍNEZ MARTÍNEZ, R., "Protección de datos, comentarios al desarrollo del Reglamento de la LOPD", Tirant Lo Blanc, 2008.

"*Una aproximación crítica a la autodeterminación informativa*", Thomson-Civitas, Madrid, 2004.

"Tecnologías de la Información, Policía y constitución*",* Tirant lo Blanch, Valencia, 2001.

MARTÍNEZ DE PISÓN CAVERO, "El derecho a la intimidad en la jurisprudencia constitucional", Civitas, Madrid, 1993.

MARTÍNEZ-ROJAS, A., "Principales aspectos del consentimiento en el Reglamento general de protección de datos de la Unión Europea", en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 42, septiembre-diciembre 2016.

MATIA PORTILLA, F.J., "La protección de los derechos fundamentales en la Unión Europea", Civitas, Madrid, 2002.

MERCHÁN MURILLO, A., y TORRALBO CARMONA, A., "Proyecto EpSOS: una sanidad electrónica transfronteriza en Europa", *Revista General de Derecho Administrativo*, nº 48, mayo 2018.

MESTRE DELGADO, J.F., "El derecho de acceso a archivos y registros administrativos (Análisis del artículo 105.b) de la Constitución)", Civitas, Madrid, 1993.

MESSIA DE LA CERDA BALLESTEROS, J.A., "La Cesión o Comunicación de Datos de Carácter Personal", Thomson-Civitas, Madrid, 2003.

MINERO ALEXANDRE, G., "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario Jurídico y Económico Escurialense*, nº 50, 2017.

MIR PUIGPELAT, O., "El acceso a la información pública en la legislación española de transparencia: crónica de un cambio de paradigma", *Revista Catalana de Derecho Público*, nº 55, diciembre 2017.

MONTALVO JÄÄSKELÄINEN, F., "Límites a la autonomía de voluntad e instrucciones previas: un análisis desde el derecho constitucional", Vol.20, nº1, V/Lex, 2010.

MORETÓN TOQUERO, A., "Transparencia, acceso a la información pública y buen gobierno. Análisis de la cuestión tras la Ley 19/2013", *Revista Jurídica de Castilla y León*, nº 33, 2014.

"Los límites del derecho de acceso a la información pública", *Revista Jurídica de Castilla y León*, nº 33, mayo 2014.

MURILLO DE LA CUEVA, P.L., y PIÑAR MAÑAS, J.L., "El derecho a la autodeterminación informativa", Fundación Coloquio Jurídico Europeo, Madrid, 2009.

MURILLO DE LA CUEVA, P.L., "Las vicisitudes del derecho de la protección de datos personales*", Revista Vasca de Administración Pública,* Vol. Nº58, 2000.

"El derecho a la autodeterminación informativa y la protección de datos personales", *Azpilcueta. Cuadernos de Derecho* (20), San Sebastián, 2008.

"Informática y protección de datos personales (estudios sobre la Ley Orgánica 5/1992, de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal)", *Cuadernos y Debates, Centro de Estudios Constitucionales,* Madrid, 1993.

"El derecho a la autodeterminación informativa y la protección de datos personales", *Sociedad de Estudios Vascos,* San Sebastián, 2008.

NIETO GARRIDO, E., *"Derecho a indemnización y responsabilidad"* Carácter en el Reglamento General De Protección de Datos hacia un nuevo modelo europeo de protección de datos. Obra colectiva dirigida por José Luis Piñar Mañas, REUS, Madrid, 2016.

"Transparencia y acceso a los documentos versus derecho a la protección de datos de carácter personal en la reciente jurisprudencia del TJUE", en *Transparencia, acceso a la información y protección de datos*, PIÑAR MAÑAS (Dir.), Reus Ediciones, Madrid, 2015.

PALACIOS, J. M., "Hacia la reforma de la Ley de Secretos Oficiales de 1968. Análisis GESI/Universidad de Granada". Disponible en:

http://www.seguridadinternacional.es/?q=es/content/hacia-la-reforma-de-la-ley-de-secretos-oficiales-de-1968.

PÉREZ VELASCO, M.M. "Los Ficheros Públicos, Estudios sobre Administraciones Públicas y Protección de Datos Personales*", Encuentro entre Agencias Autonómicas de Protección de Datos Personales".* Thomson-Civitas y APDCM, Madrid, 2006.

PIÑAR MAÑAS, J.L., y RECIO GAYO, M., "El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea", Edit. La Ley-Wolters Kluwer, Madrid, 2018.

PIÑAR MAÑAS, J.L., "Transparencia y protección de datos. Una referencia a la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información y buen gobierno", en *Transparencia, acceso a la información y protección de datos*, PIÑAR MAÑAS (Dir.), Reus Ediciones, Madrid, 2015.

PIÑAR MAÑAS, J.L. y otro, "Legislación de protección de datos", 2ª edic., Edit. Iustel, Madrid, 2011.

"Jornadas ENATI sobre el "Nuevo Reglamento Comunitario sobre Protección de Datos", CGAE, Madrid, 29 de abril de 2016.

"Código de Protección de Datos", La Ley, Madrid, 2019.

"Revolución tecnológica, Derecho Administrativo y Administración Pública. Notas preliminares para una reflexión", en *La autorización administrativa. La Administración electrónica. La enseñanza del Derecho Administrativo. Actas del I Congreso de la Asociación Española de Profesores de Derecho Administrativo,* Aranzadi, 2007.

"Protección de datos: origen, situación actual y retos para el futuro", en *El derecho a la autoderminación informativa,* Fundación Coloquio Jurídico Europeo, Madrid, 2009.

"Concepto de dato personal", en "Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal", TRONCOSO REIGADA, A., (Coord.) Civitas, Madrid, 2010.

PUENTE ESCOBAR, A., "La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal". *Azpilicueta. Cuadernos de Derecho,* San Sebastián, 2008.

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

RALLO LOMBARTEI, A., "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018), *Revista de Derecho político,* nº 100, 2017.

RAMS RAMOS, L., "El derecho fundamental a la protección de datos de carácter personal como límite ¿(in)franqueable? para la transparencia administrativa", Estudios de Deusto, Vol. 66/2, julio-diciembre 2018, págs. 119-152. Accesible en: http://www.revista-estudios.deusto.es/.

RAMS RAMOS, L., "El Derecho de acceso a archivos y registros administrativos", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad,* PIÑAR MAÑAS, J.L. (Dir.), Reus Ediciones, Madrid, 2016.

RAMS RAMOS, L., "Tratamiento y acceso del público a documentos oficiales", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad,* PIÑAR MAÑAS, J.L. (Dir.), Reus Ediciones, Madrid, 2016.

"El derecho de acceso a archivos y registros administrativos", *Colección de Derecho Administrativo*, Madrid, 2008.

"Transparencia administrativa y protección de datos personales. V encuentro de Agencias Autonómicas de protección de datos personales.", Agencia de Protección de Datos de la Comunidad de Madrid, Thomson-Civitas, Madrid, 2008.

RAZQUIN LIZARRAGA, J.A., "Acerca de la naturaleza del acceso a la información pública (A propósito de la STEDH de 28 de noviembre de 2013)", *Revista Aranzadi Doctrinal*, nº 11/2014, Aranzadi, 2014.

RECIO GAYO, M., "Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a las autoridades de control", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad*, PIÑAR MAÑAS, J.L. (Dir.), Reus Ediciones, Madrid, 2016.

REDACCIÓN THOMPSON-REUTERS ARANZADI, "La protección de datos en el ámbito sanitario", Pamplona, 2019.

REDACCIÓN MÉDICA, 12 de noviembre de 2019. Accesible en: https://www.redaccionmedica.com/

REY MARTÍNEZ, F., "Quod omnes tangit ab omnibus cognitum esse debet: El derecho de acceso a la información pública como derecho fundamental", Revista Jurídica de Castilla y León, nº 33, mayo de 2014.

RODRÍGUEZ SANTIAGO, J.M., "La ponderación de bienes e intereses en el Derecho Administrativo", Marcial Pons, Madrid, 2000.

RUBIO LLORENTE, F., "Mostrar los derechos sin destruir la Unión", *Revista española de derecho constitucional*, Año nº 22, Nº 64, 2002.

SÁNCHEZ BRAVO, A.A., "La protección del derecho a la libertad informática en la Unión Europea", Universidad de Sevilla, Secretariado de Publicaciones, Sevilla, 1982.

SÁNCHEZ-CARO, J., "Principios de la protección de datos: el uso y acceso a la historia clínica electrónica (HCE) y la protección de datos", en "Comentario a la Ley

Orgánica de Protección de Datos de Carácter Personal", Troncoso Reigada (Coord.), Civitas, Madrid, 2010.

SÁNCHEZ-CARO, J. y ABELLÁN, F, "Datos de salud y datos genéticos", Derecho Sanitario Asesores, Granada, 2004.

SÁNCHEZ GÓNZALEZ, I., "Informe sobre instrucciones previas", MARTÍN SÁNCHEZ. I., (coord.), Consejería de Sanidad, Comunidad de Madrid, 2005.

SÁNCHEZ MORÓN, M., "El principio de participación en la Constitución Española", *Revista de Administración Pública,* nº 89, 1979.

SÁNCHEZ URRUTIA, A.V., "Información genética, intimidad y discriminación", *Acta Bioética*, vol.8, nº 2, 2002.

SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, M., "Un derecho fundamental a acceder a la información pública", en *El derecho de acceso a la información pública, Actas del Seminario Internacional Complutense*, Madrid, 2008.

SANZ CALVO, L. y LESMES SERRANO, C., "Calidad de los datos; La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia", Lex Nova, Valladolid, 2008.

SANZ SALGUERO, J., "Relación entre la protección de datos personales y el derecho a la pública en el marco del derecho comparado", *Revista Ius et Praxis*, año 22, nº 1, 2016.

SARRATO MARTÍNEZ, L., "*Revista Jurídica de Castilla y León*", nº 17, enero 2019.

SERRANO PÉREZ, M.M., "El derecho fundamental a la protección de datos: su contenido esencial", en *Revista anuario multidisciplinar para la modernización de las administraciones públicas*, nº1, 2005.

"El derecho fundamental a la protección de datos. Derecho español y Comparado", Aranzadi, Pamplona 2004.

SERRANO RUIZ-CALDERÓN, J.M., "Retos jurídicos de la Bioética", Ediciones Internacionales Universitarias, Madrid, 2005.

SEVILLANO,E.: https://elpais.com/politica/2018/06/20/actualidad/1529505765_330795.html

SINDIC DE GREUGES DE CATALUÑA, "El derecho de acceso a la información pública", Informe extraordinario, marzo 2012.

SOTO LOSTAL, S., "El derecho de acceso a la información, el Estado Social y el buen gobierno", Tirant Lo Blanch, Valencia 2011.

STEINMEYER ESPINOSA, A., "¿Permite el derecho de acceso a la información pública, el acceso a datos personales?, Universidad Tecnológica Metropolitana, *Serie Bibliotecología y Gestión de Información* N° 79, Chile, 2013.

SUÁREZ RUBIO, M.J., "Constitución y privacidad sanitaria", Tirant Lo Blanc, Valencia, 2017.

SUBIRANA DE LA CRUZ, S., "Open Governement: transparencia administrativa, derecho de acceso a la información pública, "open data" y reutilización de la información del sector público", *Revista Aranzadi Doctrinal*, nº 2/2016, Editorial Aranzadi, 2016.

THE CONVERSATION: https://theconversation.com/por-que-es-tan-dificil-reutilizar-nuestros-datos-de-salud-en-investigacion-113092

TORREGROSA VÁZQUEZ, J.,"Sociedad Digital y Derecho".Directores Tomás de la Quadra Salcedo y José Luis Piñar Mañas Coordinadores Moisés Barrio Andrés y José Torregrosa Vázquez Boletín Oficial del Estado Ministerio de Industria, Comercio y Turismo y RED.ES.

TRAVERSI, A., "*II Diritto dell, informática*", Seconda edizione, Ipsoa Informáticas, 1990.

TRONCOSO REIGADA, A., La protección de datos personales, en busca del equilibrio, Tirant Lo Blanc, Valencia, 2010.

"Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal", Civitas, Madrid, 2010.

"Comentario a la ley de protección de datos, comentario al art.12 LOPD" en *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2010.

"La protección de datos sanitarios: La confidencialidad de la historia clínica, Protección de datos personales para servicios sanitarios públicos", Agencia de Protección de Datos de la Comunidad de Madrid, 2008.

"Transparencia administrativa y protección de datos personales, V Encuentro entre Agencias Autonómicas de Protección de Datos Personales", Thomson-Civitas y APDCM, Madrid, 2006.

VARIOS AUTORES "Estudios de protección de datos de carácter personal en el ámbito de la salud", Marcial Pons, 2007.

VIZCAÍNO CALDERÓN, M., "Comentarios a la Ley Orgánica de Protección de Datos", Civitas, Madrid, 2001.

ZABÍA DE LA MATA, J., y otros, "Protección de datos. Comentarios al Reglamento", Lex Nova, Valladolid, 2008.