

UNIVERSIDAD AUTÓNOMA DE MADRID

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO PÚBLICO Y FILOSOFÍA JURÍDICA

PROGRAMA DE DOCTORADO EN DERECHOS FUNDAMENTALES

ÁREA DE DERECHO ADMINISTRATIVO

2012



EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE LOS DATOS PERSONALES: ANÁLISIS DE
LOS DATOS DE SALUD EN LA HISTORIA CLÍNICA

TESIS DOCTORAL

Ángel Raúl Hernández Rodríguez

Directora: Dra. Doña Mónica Domínguez Martín

“La utopía está en el horizonte. Me acerco dos pasos; ella se aleja dos pasos. Camino diez pasos y el horizonte se aleja diez pasos más allá. Por mucho que yo camine, nunca la alcanzaré. ¿Para qué sirve la utopía? Para eso sirve: para caminar”.

Eduardo Galeano

A Dios, por darme la oportunidad de la vida y la fuerza para hacer este sueño una realidad.

A mi madre, Doña Rufina Rodríguez, por tu apoyo incondicional y comprenderme en los momentos más difíciles.

A Doña Verónica García Morales y a todos mis compañeros y amigos, por estar junto a mí durante estos años de estudio y recogimiento en la biblioteca, nunca estuve solo.

A la Dra. Mónica Domínguez Martín, por aceptarme para realizar esta tesis bajo su dirección. Su apoyo y confianza en mi trabajo y su capacidad de guiar mis ideas han contribuido rotundamente en el logro de esta meta académica.

A todos, gracias...

ABREVIATURAS UTILIZADAS

SÍMBOLO	SIGNIFICADO
AAP	Auto de la Audiencia Provincial
AAPP	Audiencias Provinciales
AEPD	Agencia Española de Protección de Datos
Art.	Artículo
Arts.	Artículos
CC AA	Comunidades Autónomas
CCE	Código Civil Español
CD Rom	Compact disc-read only memory / disco compacto de memoria sólo legible (no admite escritura).
CE	Constitución Española
CEDHyLF	Convenio Europeo para la protección de los derechos humanos y libertades fundamentales
Cfr.	Con referencia
Coord.	Coordinador
CPE	Código Penal Español
CPEA	Código Penal Español Anterior
DCP	Dato de Carácter Personal
Dir	Director
Directiva 95/46/CE, del PE y el CUE	Directiva 95/46/CE, del Parlamento Europeo y el Consejo de la Unión Europea
DNI	Documento Nacional de Identidad
Edit	Editorial
Et al	Y otros

Etc.	Etcétera
Fj.	Fundamento jurídico
L.O.	Ley Orgánica
LECiv	Ley de Enjuiciamiento Civil
LEcrim	Ley de Enjuiciamiento Criminal
LGS 14/1986	Ley General de Sanidad 14/1986, de 25 de abril
LOAP 41/2002	Ley Orgánica de Autonomía del Paciente 41/2002, de 14 de noviembre
LOPD 15/1999	Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre
Núm.	Número
Op. Cit.	Obra citada
P.	Página
PE y CUE	Parlamento Europeo y Consejo de la Unión Europea
PIB	Producto Interno Bruto
pp.	Páginas
RD	Real Decreto
s.	Siglo
SAP	Sentencia de la Audiencia Provincial
SIDA	Síndrome de Inmuno Deficiencia Adquirida
SJP	Sentencia de Juzgado de lo penal
Ss	Siguientes
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo
STSJ	Sentencia del Tribunal Superior de Justicia
TEDH	Tribunal Europeo de Derechos Humanos
Vid infra	Véase abajo

Vid supra

Véase arriba

Vid.

Véase

VIH

Virus de Inmunodeficiencia Humana

ÍNDICE

Introducción.....	12
Capítulo 1. La protección de los datos personales.....	17
1. Aproximación al tema.....	18
2. Normativa internacional.....	25
2.1. Convenio Nº 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.....	29
2.2. La Directiva 95/46/CE, del Parlamento Europeo y el Consejo de la Unión Europea, 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.....	31
3. La protección de datos en España: configuración Constitucional.....	33
3.1. La protección de datos personales en la Constitución Española.....	33
3.2. La Sentencia 292/2000 del Tribunal Constitucional Español: reconocimiento a la protección de datos como un derecho autónomo.....	39
4. Normativa estatal de protección de datos personales.....	46
4.1. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LOARTAD).....	47
4.2. Ley Orgánica de Protección de Datos (LOPD) 15/1999, de 13 de diciembre, de protección de datos de carácter personal y su reglamento, el Real Decreto 1720/2007 de 21 de diciembre.....	48
4.3. Excepciones a la LOPD 15/1999, de 13 de diciembre.....	51
4.3.1. Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.....	52
4.3.2. Los ficheros sometidos a la normativa sobre protección de	

materias clasificadas.....	54
4.3.3. Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.....	55
4.3.4. Los libros bautismales.....	56
4.3.5. Las personas jurídicas.....	59
4.3.6. Las personas fallecidas.....	59
5. Identificación y configuración de los datos de carácter personal protegidos por la LOPD 15/1999.....	60
5.1. La identificación del titular de los datos.....	60
5.2. El interesado o afectado.....	63
5.3. El responsable del fichero y el encargado del tratamiento.....	64
5.4. Obligaciones del responsable del fichero.....	69
5.4.1. Inscripción del fichero.....	71
5.4.2. Informar y obtener el consentimiento del titular de los datos.....	74
5.4.3. El consentimiento del interesado en el uso de sus datos.....	87
5.4.4. El deber de secreto.....	91
5.4.5. Establecer las medidas de seguridad.....	94
5.5. Principios en la protección de datos de salud.....	97
5.5.1. Principio de lealtad.....	99
5.5.2. Principio de proporcionalidad.....	100
5.5.3. Principio de finalidad.....	104
5.5.4. Principio de exactitud o veracidad.....	105
5.5.5. Principio de conservación.....	112
6. Regulación autonómica de la protección de los datos personales.....	113
6.1. La Comunidad Autónoma de Madrid.....	113
6.2. La Comunidad Autónoma de Cataluña.....	114
6.3. La Comunidad Autónoma del El País Vasco.....	116
7. Resumen de ideas.....	118

Capítulo 2. Los datos de salud.....	120
1. Aproximación al tema.....	120
2. Marco normativo aplicable a los datos de salud.....	122
2.1. Normativa comunitaria.....	122
2.2. Legislación estatal en materia de salud.....	126
2.3. Otras normas protectoras de los datos de salud.....	131
3. La protección de los datos de salud.....	132
3.1. Definición del dato de salud.....	137
3.2. Datos especialmente protegidos.....	140
3.3. Datos de salud del menor de edad.....	144
3.4. El dato de salud y las nuevas tecnologías.....	154
3.5. Los datos de salud – genéticos.....	160
4. Obligación de disociar el dato salud.....	163
4.1. El esfuerzo desproporcionado.....	168
4.2. La opinión del paciente para disociar el dato de salud.....	169
4.3. Obligación de disociar para investigación.....	170
4.4. Obligación de disociar para casos judiciales.....	172
4.5. Obligación de disociar para docencia.....	174
5. El consentimiento para el uso de los datos de salud.....	175
5.1. Revocación del consentimiento: un derecho del paciente a decir no.....	180
5.2. Excepciones al consentimiento en el uso del dato de salud.....	182
5.2.1. Excepciones al consentimiento y uso de datos de salud del trabajador.....	186
5.2.1.1. El reconocimiento para evaluar los efectos de las condiciones de trabajo sobre la salud.....	189
5.2.1.2. Reconocimiento para comprobar si el estado de salud del trabajador constituye un peligro para su integridad, la de sus compañeros o terceros.....	190

5.2.1.3. Reconocimientos obligatorios por disposición legal.....	191
6. Índice cumplimiento de la protección de datos de salud.....	194
7. Resumen de ideas.....	195
Capítulo 3. Los datos de salud en la historia clínica.....	198
1. Aproximación al tema.....	198
2. La historia clínica.....	200
2.1. La regulación de la historia clínica.....	207
2.2. Antecedentes jurídicos de la historia clínica.....	209
2.3. Aprobación de la LOAP 41/2002.....	213
2.4. Finalidad de la historia clínica.....	216
2.5. Características de la historia clínica.....	217
2.6. La titularidad en la historia clínica.....	221
2.6.1. Del paciente.....	223
2.6.2. Del médico.....	225
2.6.3. De la Administración.....	227
2.6.4. Posición ecléctica e integradora.....	228
2.7. Acceso a la historia clínica.....	229
2.7.1. Acceso a la historia clínica por el paciente.....	231
2.7.2. Acceso a la historia clínica por el médico.....	236
2.7.3. Acceso a la historia clínica por los familiares y terceros.....	237
2.7.4. Acceso a la historia clínica por otros profesionales.....	239
2.8. De la cancelación de datos en la historia clínica.....	240
2.9. Conservación de la historia clínica.....	241
2.10. La historia clínica informatizada.....	243
2.11. Naturaleza jurídica de la historia clínica y su validez probatoria en procesos judiciales.....	246
3. Resumen de ideas.....	247

Capítulo 4. La protección de los datos y su vinculación con la intimidad.....	250
1. Aproximación al tema.....	250
2. Concepto de intimidad.....	252
2.1. Marco constitucional - derecho de intimidad del paciente.....	263
2.2. Desarrollo de la protección constitucional.....	271
2.3. Tipos de intimidad.....	272
2.3.1. La intimidad corporal.....	273
2.3.2. Otras formas de posible intromisión a la intimidad.....	278
2.3.3. La intimidad económica.....	279
3. De la revelación de secretos.....	280
4. Protección de la intimidad en el código penal español.....	285
5. Resumen de ideas.....	288
Capítulo 5. Medios para proteger los datos de salud del paciente.....	291
1. Aproximación al tema.....	291
2. Los derechos de acceso, rectificación, cancelación y oposición.....	293
2.1. El derecho de acceso.....	296
2.1.1. El estado de necesidad terapéutica.....	310
2.1.2. Otro tipo de accesos.....	317
2.2. La rectificación.....	318
2.3. La cancelación.....	323
2.4. El derecho de oposición.....	330
2.5. Los derechos arco y los herederos del paciente.....	337
3. La obligación de callar los datos de salud.....	340
3.1. ¿Es necesario el secreto médico?.....	343
3.2. Fundamento histórico del secreto profesional.....	346
3.3. Criterios que le dan fundamento.....	348
3.4. Bases legales para el secreto médico.....	350
3.5. Límites al secreto médico.....	352

3.6. Excepciones al secreto médico.....	354
3.6.1. Consentimiento del paciente.....	354
3.6.2. Autorización de la ley.....	357
3.6.3. La declaración de enfermedades.....	361
3.6.4. El registro de nacimientos y defunción.....	363
3.6.5. Revelar el secreto a favor del paciente o de un tercero.....	363
3.6.6. Revelación en favor del propio médico.....	365
3.7. El secreto y el médico de la empresa.....	366
3.8. El secreto y el médico forense.....	367
3.9. Diferencias entre el secreto profesional del médico y el secreto profesional del abogado.....	368
3.10. La revelación de secretos en el Código Penal español, artículo 199.....	370
4. Resumen de ideas.....	379
Conclusiones.....	380
Bibliografía.....	401

INTRODUCCIÓN

El presente trabajo de investigación tiene por objeto el estudio detallado de la Protección de los Datos Personales y hace énfasis en los Datos de Salud, su reflejo en el derecho positivo, nacional e internacional, la relevancia que tiene este tipo de información en su titular y la forma en que se vincula este derecho esencial con otros derechos fundamentales reconocidos por la legislación española.

Para lograr estos objetivos, se empieza por analizar el alcance de los datos personales, destacando la importancia que tienen para el ciudadano, especialmente por los constantes controles a los que se ve sometido, por parte del Estado y los particulares.

En el transcurso de la investigación veremos que los datos que genera una persona son variados y, dependiendo de la información que encierran, pueden clasificarse como datos personales ordinarios o datos personales sensibles. Los datos personales sensibles, a diferencia de los primeros, reciben mayor protección por parte de la ley y se restringe su tratamiento sólo a personas debidamente autorizadas. En esta categoría se encuentran, los datos religiosos, los de origen racial, los de identidad sexual, los de política y los datos de salud, entre otros.

Es por esta razón que la investigación continúa su recorrido eligiendo los datos sensibles como columna vertebral de su estudio y, de entre ellos, los datos de salud, debido a la gran importancia que le asigna la LOPD 15/1999 y el impacto que genera en el paciente, si se comenten irregularidades en su uso.

En ese orden de ideas, aunque existen diversas formas de archivar los datos de salud y múltiples ficheros que contienen esta materia, la investigación se centra en la historia clínica, como el elemento más emblemático de conservación de datos de salud. Esta elección

no es a la ligera y tiene su fundamento en la obligación que establece la ley de constituir una historia clínica por cada paciente, con el fin de garantizar un tratamiento adecuado a su enfermedad.

De igual forma, al adentrarse en las características de la historia clínica, se hace evidente que en sus páginas no sólo se protege el derecho a los datos personales, también existe gran vinculación con otros derechos, como son: la intimidad, la dignidad, la salud y finalmente el derecho a la vida.

Siendo así, esta investigación también se interesa en conocer la relación que existe entre el derecho a la Protección de los Datos Personales y el Derecho a la Intimidad. Esta estrecha relación también encuentra fundamento en la historia del Derecho, ya que durante mucho tiempo llegó a decirse que el Derecho Fundamental a la Intimidad abarcaba todo lo referente a la protección de los datos, pero tal posición ha cambiado con el avance de los años, y ahora, aunque se reconoce gran vinculación entre ellos, se estima que el Derecho Fundamental a la Protección de los Datos es autónomo y con identidad individual.

Como último elemento, esta investigación hace un análisis de las alternativas que tiene el paciente, para proteger sus datos personales, desde la LOPD 15/1999 y la LOAP 41/2002, pasando por las obligaciones éticas de los profesionales de la medicina y, de manera muy somera, la cobertura que da el Derecho Penal ante la comisión del delito de revelación de secretos.

Visto lo anterior, se inicia la investigación con el análisis de los datos personales, como elemento básico para formar perfiles de las personas, se pasa por una descripción de la legislación actual que rige en esta materia, y en el Primer Capítulo (LA PROTECCIÓN DE LOS DATOS PERSONALES), se empieza por hacer un recorrido en la evolución que ha tenido este derecho a través de los años, su aprobación jurisprudencial y los diferentes tipos de datos personales que se protegen. En este primer tema, se muestra el gran debate que existe en

relación con la autonomía del derecho fundamental a la protección de los datos, su origen legal tan discutido y analizado por juristas y tribunales, en especial por su reconocimiento desde la constitución en el artículo 18.4. Ante el gran debate generado por su independencia de otros derechos, aun se le reprochan múltiples errores a este nuevo derecho fundamental, sobre todo porque su contenido aun guarda gran vinculación con el derecho a la intimidad, lo que hace que su identidad sea cuestionada y se le califique como un elemento accesorio a otros derechos fundamentales ya existentes en la carta magna.

Con base a los distintos tipos de datos que existen, se elige continuar la investigación con un tipo de datos en especial, por eso en el Capítulo Segundo (LOS DATOS DE SALUD), se hace un análisis del concepto dato de salud, el reconocimiento que este tipo de dato ha tenido al nivel internacional y estatal, y la importancia del consentimiento para su recolección previo al tratamiento. La ley ha sido muy cuidadosa con este tipo de información y ha reglamentado con detalle las obligaciones que sobrevienen al responsable del fichero, por el uso de esta información, además que, como custodio de la información, también está obligado a responder, no solo ante el dueño de los datos, sino ante los tribunales, por la forma como conserva la información y la protege de la intervención ilegal de otras personas.

En el Tercer capítulo (LOS DATOS DE SALUD EN LA HISTORIA CLÍNICA), se continúa con el análisis de los datos de salud incluidos en este documento, destacando primero el concepto de historia clínica, la reglamentación que existe actualmente y el intenso debate que subsiste sobre cómo construirla, a quién pertenece, cuál es su vigencia y qué funciones cumple para las partes involucradas. En este capítulo, se hace un análisis de los intereses de los médicos, de los pacientes y de los centros hospitalarios, por mantener en reserva la información que poseen y sobre todo, por los derechos más importantes que pueden existir en estos documentos, la Protección de los Datos y la Intimidad.

Dado que en los tres primeros capítulos se menciona mucho el derecho a la intimidad, como derecho fundamental muy vinculado a la protección de los datos, continuamos en el Capítulo Cuarto (LA PROTECCIÓN DE LOS DATOS Y SU VINCULACIÓN CON LA INTIMIDAD), con un análisis sobre este derecho y la forma como se reconoce su existencia en la Constitución Española. En este capítulo presentan las diferencias que existen entre el derecho a la intimidad y otros términos “parecidos”, generalmente utilizados para referirse a aquello que una persona mantiene en reserva. En cuanto al propio paciente, este derecho es de gran importancia, pues desde su ingreso a un hospital o centro sanitario se ve sometido a múltiples procedimientos en los que la desnudez del cuerpo y de la mente es lo primero que se le exige para lograr entender su padecimiento y proceder a la cura de su enfermedad. A pesar de ello, esta investigación también reconoce que existen otros derechos muy vinculados con la protección de los datos como son: el derecho fundamental a la dignidad y la vida, pero opta por hacer un corto énfasis en la intimidad, por su gran cercanía con los derechos del paciente.

En este orden de ideas, a lo largo de esta investigación se hizo evidente la necesidad de conocer las alternativas que quedan al paciente para proteger su información de salud y es por ello que en el último tema de este trabajo denominado, Capítulo Quinto (MEDIOS PARA PROTEGER LOS DATOS DE SALUD DEL PACIENTE), se analizan los derechos de acceso, rectificación, cancelación y oposición, también conocidos como derechos ARCO. En este capítulo, se investiga con mayor detalle el derecho de acceso que tiene el paciente y otros interesados en esta materia, asimismo, la autorización que la ley otorga excepcionalmente al médico, para ocultar, por necesidad terapéutica, información a su paciente. Aquí también se plantea la necesidad de evaluar las alternativas que quedan a los familiares o herederos de un paciente fallecido para ejercitar estos llamados derechos ARCO. Aunque está plenamente aceptado que tales derechos están unidos a la personalidad de la persona y se extinguen con su muerte, se plantea la idea de una interpretación amplia, comparada con el derecho a la Intimidad Familiar, que años antes ya han reconocido los tribunales de justicia en España.

Por otro lado se analiza la obligación más antigua que se conoce en esta área de atención al paciente, el secreto del médico, el cual inició más como un juramento ético y ha pasado a ser toda una estructura de comportamiento que define al profesional de la medicina. Este secreto médico, más desarrollado en códigos deontológicos, exige que este profesional calle la información que posee sobre el enfermo por encima de cualquier presión. Sin embargo, para la ley, este derecho del médico no es absoluto y, conforme a condiciones muy precisas, está obligado a denunciar, en su propio favor o en el de tercero, algunos aspectos que pudiese conocer sobre la salud y el comportamiento de su paciente.

Ya en el final de esta investigación, también se analiza la violación del deber de secreto y se prefiere mostrar el desarrollo desde la normativa penal, con el delito de revelación de secreto, haciendo algunos comentarios sobre la regulación que la ley ha hecho en esta materia.

CAPITULO 1

LA PROTECCIÓN DE LOS DATOS PERSONALES

SUMARIO: 1. Aproximación al tema. 2. Normativa internacional. 2.1. Convenio N° 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. 2.2. La Directiva 95/46/CE, del Parlamento Europeo y el Consejo de la Unión Europea, 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. 3. La protección de datos en España: configuración Constitucional. 3.1. La protección de datos personales en la Constitución Española. 3.2. La Sentencia 292/2000 del Tribunal Constitucional Español: reconocimiento a la protección de datos como un derecho autónomo. 4. Normativa estatal de protección de datos personales. 4.1. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LOARTAD). 4.2. Ley Orgánica de Protección de Datos (LOPD) 15/1999, de 13 de diciembre, de protección de datos de carácter personal y su reglamento, el Real Decreto 1720/2007 de 21 de diciembre. 4.3. Excepciones a la LOPD 15/1999, de 13 de diciembre. 4.3.1. Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. 4.3.2. Los ficheros sometidos a la normativa sobre protección de materias clasificadas. 4.3.3. Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. 4.3.4. Los libros bautismales. 4.3.5. Las personas jurídicas. 4.3.6. Las personas fallecidas. 5. Identificación y configuración de los datos de carácter personal protegidos por la LOPD 15/1999. 5.1. La identificación del titular de los datos. 5.2. El interesado o afectado. 5.3. El responsable del fichero y el encargado del tratamiento. 5.4. Obligaciones del responsable del fichero. 5.4.1. Inscripción del fichero. 5.4.2. Informar y obtener el consentimiento del titular de los datos. 5.4.3. El consentimiento del interesado en el uso de sus datos. 5.4.4. El deber de secreto. 5.4.5. Establecer las medidas de seguridad. 5.5. Principios en la protección de datos de salud. 5.5.1.

Principio de lealtad. 5.5.2. Principio de proporcionalidad. 5.5.3. Principio de finalidad. 5.5.4. Principio de exactitud o veracidad. 5.5.5. Principio de conservación. 6. Regulación autonómica de la protección de los datos personales. 6.1 La Comunidad Autónoma de Madrid. 6.2. La Comunidad Autónoma de Cataluña. 6.3. La Comunidad Autónoma del El País Vasco. 7. Resumen de ideas.

1. Aproximación al tema.

Con el paso del tiempo las técnicas para acumular información acerca de las personas fue mejorando notablemente y la capacidad de archivar y organizar documentos se hizo cada vez más fácil, tanto para el Estado, como para los particulares.

El desarrollo de las nuevas tecnologías, en especial de los sistemas y medios informáticos y telemáticos, está provocando nuevos e interesantes problemas jurídicos. Las publicaciones en la prensa y los estudios doctrinales recientes se refieren a distintos conflictos con la protección de los datos, por el uso de estas herramientas tecnológicas, en los más diversos ámbitos de la vida de los ciudadanos. Así pues, como señala ORDÓÑEZ SOLÍS “nunca como ahora y en las sociedades democráticas se había gozado de más libertad, pero también debido a los adelantos tecnológicos jamás las amenazas a la libertad y los riesgos de invadir nuestro ámbito privado habían sido tan preocupantes¹”. La idea del autor concuerda perfectamente con la tendencia del día a día de la sociedad actual, ya que las nuevas herramientas informáticas han hecho del mundo un lugar pequeño y poco o nada escapa del control o la vigilancia de algunas personas.

¹ ORDÓÑEZ SOLIS, David, Privacidad y protección judicial de los datos personales, Bosh, 2011, p 14. En esta obra el autor critica la forma tan “ligera” con la que se trata el derecho a la intimidad en estos días, la manera tan abierta como los particulares comercializan este derecho y el trastoque que se da al concepto de la privacidad en los medios de comunicación, con el objetivo de vender más “primicias” a la audiencia.

CERRILLO I MARTÍNEZ nos dice que un ejemplo importante es el cambio² sufrido por las instituciones públicas, puesto que han ampliado la forma de comunicarse con los ciudadanos y ahora utilizan con mayor frecuencia la Internet, como medio para hacer pública información variada, con el propósito de llegar a la mayor cantidad de población posible. De allí que “la transición del acceso pasivo al acceso activo se ha visto potenciada por la utilización de las nuevas tecnologías de la información y la comunicación por parte de las Administraciones Públicas, ya que estas tecnologías permiten, además de la difusión en si misma, la investigación, la selección y la integración de la información, así como su presentación en un formato que pueda ser útil y comprensible a la ciudadanía³.”

La Ley 11/2007⁴, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, ya reglamentó esta realidad y mediante ella se reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas, con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

² Este cambio no sólo abarca la forma de comunicarse, sino también la forma de administrar sus propios servicios. De esta manera, en los servicios sanitarios, ahora existen nuevas modalidades de gestión en los que lo público y lo privado se mezclan y generan nuevas formas de atención a las personas. En este sentido, expone con gran detalle, DOMÍNGUEZ MARTÍN, Mónica, Formas de gestión de la sanidad pública en España, La ley, 2006.

³ CERRILLO I MARTÍNEZ, Agustí, “La difusión de información pública en internet”, en CERRILLO I MARTÍNEZ, Agustí, et al, La administración y la información, Marcial Pons, 2007,p.21

⁴ Publicada en el BOE de 23 de junio de 2007

Sobre esta ley y sus consecuencias, nos dice SÁNCHEZ NAVARRO que, “todas estas ventajas derivadas de la utilización de los medios telemáticos⁵ pueden significar también nuevas eventualidades para la privacidad de las personas, teniendo en cuenta la cantidad de datos de carácter personal (DCP) que se llegan a manejar y a interconectar en la gestión electrónica de los procedimientos administrativos, normalmente ubicados en los sitios “Web” de las AAPP que, como ha señalado la AEPD, no tienen la consideración de fuentes de acceso público”⁶. En su destacado artículo, el autor señala la importancia que tienen las nuevas tecnologías, pero no deja de lado las posibles amenazas que pueden surgir de los equipos y de sus programas informáticos, ya que la información en la red, va dejando huellas fáciles de seguir por cualquier ordenador. La mayoría de los ataques a la información no son con base a problemas tecnológicos solamente, sino por la poca seguridad que en ocasiones brindamos a los datos, desde las Administraciones Públicas, el titular de los datos y los propios usuarios en general.

Visto lo visto, los ordenadores utilizados por entes públicos y privados, cada vez más especializados y con mayor capacidad de memoria, han reemplazado a los grandes depósitos de documentación física, dando paso a los datos conservados de forma electrónica, que ahora están a disposición de muchas personas a la vez y sin límite de tiempo.

Siguiendo estas ideas, parece que no es suficiente con que las diferentes Administraciones Públicas cuenten con un servicio de información pública, también es importante garantizar que “el acceso activo de la información” sea un servicio de interés general. Es decir, no basta con la creación de infraestructuras y servicios de difusión de la

⁵ La Telemática es una disciplina científica y tecnológica que surge de la evolución y fusión de la telecomunicación y de la informática.

⁶ SÁNCHEZ NAVARRO, Álvaro, “La articulación del derecho a la protección de datos de carácter personal en la gestión electrónica de los procedimientos administrativos”, en Revista Española de Protección de Datos, Thomson Civitas, julio –diciembre, 2007, núm. 3, p.100

información (en el sentido orgánico y funcional), sino que hay otros factores que inciden en esta nueva forma de ofrecer información pública mediante Internet. Sobre el particular, resalta en esta investigación que además de lo anterior, hace falta formar al ciudadano para que conozca de éstas nuevas opciones de información y pueda utilizarlas correctamente, dirigirse oportunamente ante la autoridad y corregir aquellos datos que no sean correctos o actuales. De no hacerlo, podría traer consecuencias negativas y desencadenar una serie de problemas para si y para terceros, dados los múltiples fines que otros puedan darle a su información, sobre todo, porque las aparentes ventajas que conlleva utilizar los sistemas informáticos, exige un mínimo de seguridad física y lógica, en los sistemas y los equipos, respectivamente.

Esta nueva realidad informatizada hizo necesaria la creación de normas, nacionales e internacionales, que velasen por la protección de la información de las personas, primero resguardando su derecho a la intimidad y dignidad; y en la actualidad protegiendo su derecho a la autodeterminación informativa⁷ o libertad informática. Sobre este nuevo derecho, el Tribunal Constitucional ha reconocido que “la garantía de la intimidad, *latu sensu*, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así un 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”⁸ Para ORDÓÑEZ SOLIS “el derecho a la protección de los datos tiene

⁷ Este concepto nace en la República Federal Alemana con la sentencia dictada por el Tribunal Constitucional Federal Alemán en la sentencia sobre la Ley del Censo. En esta sentencia, el Tribunal Constitucional Federal Alemán afirmó que el derecho general de la personalidad también comporta la atribución al individuo de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar sobre su propia vida. Sobre lo anterior, Cfr. HEREDERO HIGUERAS, Manuel, “La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983”. Documentación Administrativa, N.º 198, pp. 139-158.

⁸ STC, 11 de 13 enero de 1998, FJ: 4 (RTC 1998\11)

tres dimensiones esenciales: la propia de la persona concernida por los datos, que es objeto de protección; quien tiene a su disposición los datos personales sea persona Pública o Privada y que está obligada a respetar el derecho y los poderes públicos, incluidos los jueces, encargados de proteger y amparar el derecho fundamental”⁹.

Ahora bien, antes de continuar, debemos advertir que esta investigación analiza la protección de los datos, desde su tratamiento físico o automatizado, y aunque se pueda mencionar constantemente el riesgo que implica el mal uso de la informática, tampoco sería justo eclipsar el adelanto tecnológico y a todos los equipos y programas diseñados para ayudar a resolver los problemas cotidianos, por el contrario, han sido una gran respuesta a las necesidades sociales, en especial en el ámbito de la salud, más bien, habría que señalar que “el mal uso” que las personas dan a estas herramientas es lo que ha traído como consecuencia una intensa actividad legislativa y judicial, en aras de mantener ese orden social que tanto se ve amenazado.

Los ordenadores sirven para propósitos diversos y han sido la clave para solucionar problemas muy importantes, su adaptación a los nuevos tiempos ha permitido su distribución masiva y en múltiples formas, ya no sólo tenemos el ordenador de mesa como único modelo, ahora contamos con micro procesadores (nanotecnología)¹⁰ y dispositivos portátiles, logrando una conexión y efectos mundial. Tal vez como dice BALLESTEROS MOFFA, “sólo la dimensión global desde la que hoy se contempla la libertad informática, merced a la universalidad de las comunicaciones electrónicas, justifica la necesidad de

⁹ ORDÓÑEZ SOLIS, David, Privacidad y protección judicial de los datos personales, Op. Cit., p 16

¹⁰ Nano es un prefijo griego que indica una medida (pequeña) y se habla de procesadores desarrollados con nanotecnología, porque pueden reducir su tamaño y mantener las mismas características y ventajas que las versiones de tamaño regular. Su utilización es diversa, aunque en los campos médicos destaca por su gran uso para el tratamiento de enfermedades.

regulación específica del sector”¹¹. En este sentido, el autor defiende que el problema con los datos existe desde hace mucho, y su afectación en bienes jurídicos ya es bien conocida por el derecho, pero es la magnitud de la afectación y los daños globales que se pueden causar, lo que debe motivar a la aprobación de normas específicas que regulen la protección de datos. A esto le vemos mucha lógica, pues la información personal ha existido desde que nos unimos en sociedades, pero es el alcance que esto puede tener lo que realmente alarma a la población.

En sí, el riesgo es cómo se programe un ordenador y para qué se utilice, pues no es lo mismo comparar un equipo que sirve solamente para llevar cálculos de inventario en una empresa y que ayuda enormemente al desarrollo comercial, a compararlo con equipos cuya base es una computación ubicua¹², o dedicada a obtener información, sin que nos percatemos de ello, algo que CORRIPIO GIL-DELGADO ha señalado como “tratamiento invisible, pues con este sistema, el usuario se ve privado de la posibilidad siquiera de ejercitar sus derechos”¹³. Para ČAS, “la computación ubicua supone una amenaza sin precedente no sólo para la privacidad, sino para los numerosos componentes de las sociedades liberales y democráticas para las que la privacidad desempeña un papel funcional”¹⁴.

En este sentido, el autor se refiere a aquellos equipos de informática que funcionan de forma discreta, basados en tecnologías invisibles incorporada a los entornos y artefactos del día a día, aquellos equipos que no requieren teclados y otros periféricos para

¹¹ BALLESTEROS MOFFA, Luis Ángel, La privacidad electrónica. Internet en el centro de protección, Tirant lo Blanch, 2005, p.142

¹² Tecnología de informática invasiva que, de forma imperceptible, está diseñada para captar la información que tiene a su alrededor, con propósitos de vigilancia.

¹³ CORRIPIO GIL-DELGADO, María de los Reyes, Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet, Agencia de Protección de Datos, 2000, p.134

¹⁴ ČAS, Johann, “Computación ubicua, privacidad y protección de datos: opciones y limitaciones para reconciliar contradicciones sin precedentes”, en Revista Española de Protección de Datos, núm. 6, enero – junio, 2009, p 72

incorporar nueva información a su sistema, sino que mediante una programación previa, se encargan de vigilar y procesar diversos tipos de información, entre ellas, el uso que hacen diariamente los individuos en la Internet (equipos y virus que roban contraseñas), otros encargados de vigilar los movimientos físicos de las personas, su lenguaje y demás rasgos biométricos, para generar perfiles que serán utilizados para distintos propósitos posteriormente.

Un caso muy común podría ser los ordenadores con nuevos programas de vigilancia, actualmente instalados en las terminales de aeropuerto, que se encargan de seguir, fotografiar y registrar a los viajeros mientras recorren los pasillos, sin que los mismos se percaten de tal hecho. Después, con estos “datos personales” generan ficheros que posteriormente se utilizan primordialmente para identificar posibles amenazas a la seguridad nacional. Aquí ČAS, con muy buen criterio a nuestro parecer, advierte de la violación de principios fundamentales en la protección de datos, como son el principio de Limitación de recogida de la información, el Principio de Especificación de propósito y el Principio de limitación de uso, pues sería lamentable que con el afán de promover ciertos bienes jurídicos, o utilizando conceptos como seguridad nacional, no se pongan límites al uso de la tecnología y se termine utilizando la información con propósitos perversos.

En esto, entendemos que hay peligros, y que la intención de cada individuo podría cambiar los propósitos de la invención de los procesadores de datos, convirtiéndolos en un serio peligro para el derecho de las personas. Como señala LUCAS MURILLO “un sistema centralizado de tratamiento automático de datos que no respetara límite alguno en cuanto a la información a recoger, almacenar, y transmitir, convertiría a la sociedad en una casa de cristal en la que nuestro hogar, nuestra situación financiera, nuestras relaciones, nuestra salud física y mental serían puestas al desnudo ante cualquier observador”¹⁵. En su

¹⁵LUCAS MURILLO DE LA CUEVA, Pablo, El derecho a la autodeterminación informativa la protección de los datos personales frente al uso de la informática, Tecnos, 1990, p. 108

obra, el autor reconoce que el progreso si que ha traído un instrumento extraordinariamente eficaz, tanto para lo bueno como para lo malo. Evidentemente, si no se establecen los mecanismos necesarios existirá el riesgo de una utilización retorcida con funestas consecuencias. No parece que esto sea exclusivo de los ordenadores pero, si comprendemos que esa dimensión mundial que le caracteriza provoca que los riesgos sean mucho más altos, el impacto en la persona más grave y el interés por el Estado en prevenirlo más urgente.

Si en algo estamos de acuerdo es que se hacía necesario lograr la reglamentación de las relaciones existentes entre las personas y en especial, la captación de sus datos personales, a fin de determinar las opciones legales que tiene una persona al considerar que se ha afectado su derecho, bien sea a la intimidad o bien a la propia identidad¹⁶ que le caracteriza. De allí, que se ha generado múltiple normativa internacional, precisamente para reglamentar la utilización de la información de los particulares, algunas de estas disposiciones legales han servido de semilla para la legislación interna de los estados, y su importancia ha provocado el reconocimiento de nuevos derechos y la generación de interesantes decisiones judiciales.

2. Normativa internacional.

A la vista de los elementos anteriores, se iniciaron los proyectos normativos para proteger la información. Las primeras normas fueron de carácter internacional y después, mediante aprobación interna, se trasladaron sus principios a la legislación estatal. De esta manera, en España la legislación que protege los datos surge como consecuencia de la trasposición de criterios internacionales, adaptados a la realidad del país.

¹⁶ LOPEZ GARRIDO, Diego y MARTÍN PALLÍN, José, "La informática: un riesgo incontrolado", en Revista Vasca de Administración Pública, núm. 20, 1998, p.202

Para algunos autores, entre ellos HERRAN ORTIZ, esta trasposición no fue exacta y se dejaron algunos espacios en la ley que motivaron grandes dudas con posterioridad¹⁷. La autora señala que se usaron muchos términos ambiguos. No obstante, es evidente que con el pasar de los años, aunque los términos iniciales no fueron muy precisos, si se ha logrado ajustar la normativa y acercarse mucho al interés buscado por el legislador nacional e internacional. Además, el desarrollo del derecho positivo interno Español, ha logrado ajustar con mayor precisión otros conceptos, lo que ayuda mucho a la interpretación de la norma.

Como primera referencia tenemos el artículo 12 de la Declaración Universal de Derechos Humanos que establece que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. Este documento, aprobado el 10 de diciembre de 1948 por Asamblea General de las Naciones Unidas, es de validez indiscutible para las siguientes generaciones de normas, pues deja sentado el principio del derecho a una vida privada. Ahora bien, como norma de carácter internacional, la Declaración Universal de Derechos Humanos, tiene un valor excepcional, ya que sienta las bases para otros textos normativos con iguales o parecidos propósitos.

Después de la II guerra Mundial, y los lamentables sucesos que lo acompañaron, se hizo necesario proteger con más fuerza los Derechos Humanos y las Libertades Fundamentales. Para esto, se requirió una mayor colaboración entre los Estados Europeos, por tanto, en 1949 se creó el Consejo de Europa, como un organismo internacional conformado inicialmente por 10 naciones (aunque en la actualidad esta cifra ha aumentado hasta llegar a 47¹⁸ miembros).

¹⁷ HERRAN ORTIZ, Ana, El derecho a la protección de datos personales en la sociedad de la información, Edit. Universidad de Deusto, 2003, p.90

¹⁸ Bélgica Dinamarca, Francia, Irlanda, Italia, Luxemburgo, Países Bajos, Noruega, Suecia, Reino Unido, Grecia, Turquía, Islandia, Alemania, Austria, Chipre, Suiza, Malta, Portugal, España, Liechtenstein, San Marino,

Este nuevo organismo logró, un año más tarde, la aprobación del Convenio Europeo de Derechos Humanos y Libertades Fundamentales, como un instrumento de extraordinario valor, cuyo propósito principal es proteger internacionalmente los derechos y libertades de las personas, tomando como base un catálogo de derechos que deben ser respetados por todos los países firmantes.

El Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales (CEDHyLF), con vigencia a partir de 1953, posee tres títulos fundamentales que recogen aspectos relacionados con la Declaración de los Derechos Humanos y las características que deben adoptar los diferentes gobiernos europeos. A su vez, estos títulos se dividen en 59 artículos, de los cuales destacamos el artículo 8 que señala: “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”. El Consejo de Europa ha tenido un desarrollo dinámico en este tema y, por consiguiente, ha promulgado una amplia normativa tendente a regular la protección a los datos. En sus inicios, lo hizo mediante actividad de la Asamblea parlamentaria, que desde los años setenta ha ido aprobando diversas resoluciones, recomendaciones y otros, en esta área.¹⁹

Finlandia, Hungría, Polonia, Bulgaria, Estonia, Lituania, Eslovenia, República, Checa, Eslovaquia, Rumania, Andorra, Letonia, Albania, Moldavia, Macedonia, Ucrania, Rusia, Croacia, Georgia, Armenia, Azerbaiyán, Bosnia-Herzegovina, Serbia, Mónaco y Montenegro

¹⁹ En 1968, la Asamblea parlamentaria del Consejo de Europa aprobó la Recomendación 509 en que se instaba al Comité de Ministros a aclarar si el Convenio Europeo de Derechos Humanos y demás ordenamientos nacionales eran suficientes protección para el derecho a la vida privada frente a los nuevos retos de las tecnologías. De lo anterior se comprobó que no existía tal suficiencia, lo que dio motivo a la aprobación de las Resoluciones de 1973 y 1974, ambas sobre la protección de la privacidad frente a las bases de datos en el sector público y privado. De estas resoluciones aunque fueron de gran valor, también se puede decir que al no tener mayor valor vinculante, se optó por aprobar posteriormente el Convenio 108 de 28 de enero 1981, para así lograr mayor fuerza de cumplimiento.

Este artículo 8 del CEDHyLF, ha sido analizado en repetidas ocasiones por el Tribunal Europeo de Derechos Humanos (TEDH), para así delimitar el ámbito de “esfera privada”. Esto es comprensible, ya que este término es amplio y sujeto a subjetividad, conforme a la legislación de cada país, lo que en ocasiones puede generar fuertes controversias en torno su alcance. De lo anterior, ARENAS RAMIRO comenta, “el ámbito que el Tribunal Europeo define como “esfera privada” se protege en los Estados firmantes mediante el reconocimiento de los correspondientes derechos fundamentales (derecho a la intimidad, derecho a la dignidad), que no siempre coinciden exactamente con el derecho a la vida privada y familiar reconocido en el CEDHyLF”²⁰. La autora nos señala 4 elementos fundamentales que utiliza el TEDH para conformar la esfera privada.

Inicia señalando que las comunicaciones verbales mantenidas con otros individuos son elementos propios de la vida privada y que requieren protección adicional a la vez, señala que este tipo de comunicación guarda diferencia con la escrita, debido a que ésta ya tiene una protección específica, sobre la protección a la correspondencia. Seguidamente, nos dice que fue de amplio debate si la honra, la imagen y el respeto a la reputación también se incluían en el ámbito de la esfera privada, sin embargo el TEDH ha determinado que para ciertos casos, si que constituyen parte, pues todo individuo tiene derecho a decidir de qué manera y de qué modo quiere ser representado en público. Como tercer elemento, incluye el derecho al respeto tanto del nombre propio como del apellido, pues representan parte fundamental de la identidad personal y como nexo de unión con la familia y; por último, la defensa de los datos personales, en especial los datos médicos, pues pertenecen a la vida privada de las personas.

²⁰ ARENAS RAMIRO, Mónica, El derecho fundamental a la protección de datos personales en Europa, Tirant lo Blanch, 2006, p. 55

Estos elementos, en especial el último, ha sido la base para que posteriormente los Estados y más aun sus tribunales, reconocieran la existencia de un derecho a la protección de la información. Sobre la esfera privada, tenemos que señalar, que en sus inicios se consideró que estaba compuesta por todo aquello que no se realizara en público, haciendo parecer que lo privado se reservaba sólo a lo doméstico, sin embargo, con posterioridad el Tribunal Europeo ha reconocido que las actuaciones en público no necesariamente escapan de la consideración de vida privada, más aun si se atiende a la “calidad de las personas”, por aquello que existen personas públicas, políticas²¹ u ordinarias.

2.1. Convenio N° 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

El Convenio N° 108, del Consejo de Europa, de 28 de enero de 1981²², para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, se aprobó como consecuencia de resoluciones previas²³, que cimentaron la idea de promover un convenio que garantizara los derechos de las personas a tener una vida privada, sin desatender la necesidad de armonizar este derecho con el derecho de libre circulación de

²¹ El TEDH consideró en el caso Craxi (Nº2), de 17 de julio de 2003, que cuando una figura pública se ve envuelta en un suceso público (se trataba de un caso sobre corrupción política y escuchas telefónicas que habían sido publicadas en prensa), aunque los medios de comunicación tienen el objetivo de transmitir tal información y el público tienen el derecho a recibirla, las figuras públicas (políticos en este caso), también deben tener garantizados los derechos recogidos en el art. 8 CEDH.

²² Ratificado por España en el BOE de 15 de noviembre de 1985

²³ El Consejo de Europa antes de este Convenio 108, también aprobó otras resoluciones, entre las que están la Resolución (68)509 de la Asamblea del Consejo de Europa de 1968, sobre los derechos humanos y los nuevos logros científicos y técnicos; la Resolución (73)22, de 26 de septiembre de 1973 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado; y la Resolución (74)29, de 20 de septiembre de 1974 respecto de la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público.

la información. No podemos decir que sus ordenanzas fueran de estricto cumplimiento, porque dejaba, en su artículo 4, la obligación a los países de normar estos derechos. En cuanto a la protección de datos personales, incorporó la definición de conceptos importantes, como dato personal, fichero, tratamiento automatizado y otros de especial interés.

Dentro de su redacción resaltamos el artículo 6 que establece “Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales”. Este convenio también señaló que es necesario regular el derecho a la circulación de información personal, a fin de no violar bienes jurídicos tan importantes como la intimidad o la propia vida privada de las personas. Ya desde este momento comienza a sentirse la necesidad de definir hasta dónde es necesario tutelar un derecho a la protección de datos, frente a los poderes de terceros a publicar información que no les pertenece.

Otro elemento esencial en este Convenio es establecer la calidad de los datos y hace referencia a las características que debe tener la información para poder considerarse cierta y por tanto ajustada al derecho, elementos como una información veraz, segura y obtenida con fines claros y legítimos, sirvieron de base para el desarrollo de nuevas legislaciones en materia de protección de datos. Aunque será tema de análisis posterior, si diremos desde ahora que en cuanto a los temas de salud, este convenio señala que no podrán tratarse automáticamente, salvo que los estados de manera interna, establezcan garantías apropiadas, en otras palabras, traslada la obligación a los estados de procurar medidas efectivas en la protección de este tipo de información.

Sobre la protección de datos, el Parlamento Europeo ha dictado varias directivas, entre ellas, la Directiva 95/46/CE, del PE y el CUE, de 24 de julio 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; la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones; 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 o directiva sobre la privacidad y las comunicaciones electrónicas; y la Directiva 2006/24/CE sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.

2.2. La Directiva 95/46/CE, del Parlamento Europeo y el Consejo de la Unión Europea, 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.

Dentro de las anteriores, destaco la Directiva 95/46/CE, del PE y el CUE, porque sirvió de base para actualizar la Ley 5/1992, normativa aprobada por España para regular la protección de datos y se utilizó además como base para redactar la actual LOPD 15/1999. Esta directiva, al igual que el Convenio 108, trata de establecer un punto medio entre el derecho a la protección de datos y el derecho a la libre circulación de la información. Y es que el Convenio 108, aunque tenía muchas ventajas para la época no fue de aplicación directa, lo que trajo como consecuencia la necesidad de crear una norma que así lo permitiese.

Del mismo modo, esta directiva no sólo se refirió a los datos automatizados, también incorporó a los datos tratados manualmente, lo que constituye una de sus principales características. A su vez, dado que influyó directamente en la elaboración de la LOPD 15/1999, que derogó la Ley 5/1992 conocida como LOARTAD, también fue propulsora

de la actualización del derecho positivo español. Esta directiva, incorpora otras definiciones de conceptos, tal como lo había hecho con anterioridad el Convenio 108, pero un elemento fundamental fue establecer el principio de calidad y, sobre todo, que amplía los conceptos de información al interesado y la obligatoriedad de obtener su consentimiento. No menos importante es la posibilidad de establecer el régimen de autoridades encargadas de proteger los datos.

En cuanto al tema que abordaremos posteriormente, esta directiva establece una serie de excepciones para el tratamiento de datos sensibles, entre los cuales se cuentan los datos de salud (Ver capítulo 2.), aquí menciona exenciones como: el consentimiento del afectado (Ver capítulo 2.5.), el interés vital y la obligación de secreto (Ver capítulo 5.3.), entre otros.

Por otro lado, la Carta Fundamental de los Derechos Fundamentales de la Unión Europea, en su artículo 8, establece el reconocimiento de la protección de datos de carácter personal y establece que “Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan”. Además, 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. Sobre la Carta de los Derechos Fundamentales, se aprobó una versión adaptada que fue proclamada el 12 de diciembre de 2007 en Estrasburgo, antes de la firma del Tratado de Lisboa que, una vez ratificado éste, hace la Carta legalmente vinculante para todos los países excepto Polonia y el Reino Unido.

3. La protección de datos en España: configuración constitucional.

3.1. La protección de datos personales en la Constitución Española.

Siguiendo el orden jerárquico de las normas, debemos comenzar diciendo que en España, en la Constitución de 1978, se protege el derecho a la intimidad de la personas, a través el artículo 18. Este artículo recogió además, y de manera novedosa para la época, una modalidad de protección de los datos, mediante su apartado 4, que dispuso además la “limitación” en el uso de la informática, para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Esta aprobación surge como consecuencia de la previsión tomada por los legisladores al notar la gran variedad de afectación que puede darse mediante el uso de herramientas informáticas. Algunos autores, como SUBIZA PÉREZ, han señalado que “literalmente, más que recoger un derecho lo que hace es advertir de un peligro, el uso de la informática debe ser limitado por la ley, la informática es una amenaza no solo para la intimidad personal y familiar, sino para el pleno ejercicio de los derechos de los ciudadanos”²⁴.

El autor señala también que la constitución no cita el derecho a la protección de datos, sino que, por el contrario, se refiere a la intimidad, lo que ha motivado incesantemente la pregunta si este derecho a la protección de los datos, basados en el principio constitucional, está atado al derecho fundamental a la intimidad o si se trata de un derecho autónomo. Inicialmente esta posición tuvo fundamento, debido a que si el derecho

²⁴ SUBIZA PÉREZ, Ignacio, “La construcción del derecho a la protección de los datos personales como un derecho autónomo, en SUBIZA PÉREZ, Ignacio (coord.), La protección de datos y sus mundos, publicaciones jurídicas, 2009, p.33

a la protección de datos versa sobre un derecho fundamental, se abren toda una serie de “prerrogativas”, debido a esta condición. La más inmediata es la posibilidad de presentar recurso de amparo y la de tener un proceso preferente y sumario.

De manera previa, hay que decir que hasta aquí se confundía la facultad de controlar la información personal como un derecho accesorio, que dependía directamente del derecho fundamental a la intimidad y que, en todo caso, no era un derecho autónomo, per se. Además, que sólo los datos tratados mediante sistemas informáticos serían sujetos de protección legal, pues en dicha época eran los únicos que podrían representar algún tipo de peligro para el derecho de las personas.

Tal vez, esta diferencia con el trato manual, se debía a la lentitud del sistema físico frente al sistema automatizado, lo aislado que están los datos archivados en formato papel entre sí, o su limitación en el tiempo, producto del deterioro regular de los documentos, lo que no representaba una amenaza latente para el derecho de las personas.

No obstante, la realidad que hemos vivido nos dice que el elenco de derechos humanos no es estático, por el contrario, se mantiene en constante movimiento y actualización así lo han marcado las distintas generaciones de derechos, algunos determinados por la propia realidad histórica del ser humano. Lo que nos lleva a aceptar lo señalado por PEREZ – LUÑO cuando afirma que “cada vez más se incorporan nuevos derechos a un catálogo que es permeable y abierto a la incorporación de nuevos valores y nuevos derechos²⁵. Así, las distintas generaciones de derecho humanos han surgido conforme el paso de la historia, los primeros se refieren directamente a la persona, los segundos a las personas como parte de la sociedad, y los terceros de las sociedades entre sí. Cómo podría negarse la idea de que podrían existir nuevos derechos fundamentales que,

²⁵ PEREZ – LUÑO, Antonio E., “Nuevos derechos fundamentales de la era tecnológica: libertad informática, Anuario de Derecho Público y Estudios Políticos, núm. 2.1989 – 1990, p. 176

aunque cercanos en contenido a otros derechos, mantienen una identidad que los hace diferentes e individuales al resto de derechos fundamentales.

Esta estrecha vinculación entre derecho a la intimidad y la protección de los datos permaneció durante varios años, y aunque existían posturas diversas, no se llegaba a reconocer la independencia del derecho fundamental a la protección de la información personal. Esta diferencia en el trato doctrinal se logró finalmente mediante la elaboración de jurisprudencia por el Tribunal Constitucional Español, que entre los periodos de 1993²⁶ al 2000 determinó la independencia del derecho fundamental a la protección de datos, del derecho fundamental a la intimidad. Sin embargo, destacamos la Sentencia 254/1993 de 20 de julio, pionera en esta área, la cual fue ampliamente debatida y sujeta a varias interpretaciones, pues en algunos casos se le acusaba de tener un carácter ambiguo, ya que en algunos momentos señalaba la independencia de un derecho fundamental a la autodeterminación, pero en otros parecía más partidaria de una interpretación evolutiva del derecho a la intimidad.

Esta consideración no ha sido aislada y por lo menos MARTÍNEZ MARTÍNEZ, señala que “en la práctica no parece suceder otra cosa que la existencia de la necesidad de escoger entre una vía novedosa, y brillantemente importada por la doctrina, o bien optar por una interpretación más arriesgada de un derecho fundamental preexistente, en cualquier caso, es probable que el resultado práctico sea el mismo”.²⁷ Son dos ejes, dice el autor, a los que ofrece solución esta sentencia: por un lado, el efecto en el ordenamiento jurídico interno

²⁶ STC, 254-1993, de 20 julio de 1993, FJ: 6 (RTC 1993\254) Esta sentencia señaló que 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.

²⁷ MARTÍNEZ MARTÍNEZ, Ricard, Una aproximación crítica a la autodeterminación informativa, Civitas, 2004,p.

de un Convenio Internacional²⁸ que requiere por tanto un desarrollo legislativo; y por otro, dos temas coexistentes, la determinación de “cual sea” la naturaleza jurídica del artículo 18.4 y el alcance de la tutela que el derecho a la intimidad otorga a los ciudadanos.

Tan contundente es lo expresado por DEL CASTILLO VÁZQUEZ cuando dice que “el artículo 18.4 fue tildado desde su génesis como un apéndice, una reiteración, en principio, innecesaria e injustificada, de la genérica protección que otorga el apartado 1 (art. 18.1 CE derecho fundamental a la intimidad), a los derechos tutelados en el mismo, y dice injustificada, toda vez que el constituyente no atiende en sus previsiones a las posibles invasiones producidas por el mal uso de las publicaciones escritas, las fotografías u otros medios ajenos a la informática que, de igual modo, pudieran violentar los derechos a la intimidad y al honor²⁹. En este comentario la autora señala también que otras leyes posteriores trataron de dar auxilio en este tema, y ejemplo de ello, es la cobertura solidaria que da la Ley 1/1982³⁰, de 5 de mayo, sobre protección civil al derecho al honor, la intimidad personal y la propia imagen, que apoya la materia de protección de la informática. Sin embargo, nos dice que la ayuda aportada por dicha ley no “dejó de ser un intento de encubrir la dejación del legislativo a la hora de cumplir la obligación que le impuso el constituyente para limitar, por vía legal, el uso de la informática”.

Siguiendo con los comentarios a la STC 254/1993, en ocasiones acaricia la idea de la autodeterminación, pero termina basándose en el derecho fundamental a la intimidad; peor aún, en algunos fundamentos jurídicos utilizaba ambos conceptos como similares, sin aclarar cuál es el derecho fundamental cuya tutela se pretende y en otras los consideraba

²⁸ En este aspecto se critica que, aunque el artículo 10.2 de la CE, posibilita a los convenios internacionales presidir la interpretación de los preceptos constitucionales relativos a los derechos fundamentales, esta facultad no permite que se incorporen dichas normas internacionales en el derecho positivo interno.

²⁹ DEL CASTILLO VÁZQUEZ, Isabel-Cecilia, Protección de datos: cuestiones constitucionales y administrativas – el derecho a saber y la obligación de callar, Thomson Civitas, 2007, pp.143 y 144

³⁰ Publicada en el BOE de 5 de mayo de 1982

distintos. Ya más adelante se cuestiona que en esta sentencia el Tribunal Constitucional desborda claramente los límites de la interpretación literal, acto que no es considerado ilícito, pero que si representa un riesgo.

En este mismo orden de ideas, tal como señala CONDE ORTIZ, había “algunas críticas por parte de la doctrina sobre la idoneidad de la expresión protección de datos, en cuando da a entender que se está protegiendo al dato, cuando lo que se quiere proteger es al sujeto titular de los datos”³¹. No obstante, acepta la autora que esta crítica ha sido superada, pues se perseguía centrar el alcance y contenido de la materia.

Visto así, otra destacada sentencia en esta materia, es la STC 11/1998, de 13 de enero (caso RENFE), en la que se reafirmó con mayor claridad el derecho fundamental a la autodeterminación informativa, al señalar que “no sólo entraña un específico instrumento de protección de los derechos del ciudadano, frente al uso torticero de la tecnología de la informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona”.³²

Para OROSCO PARDO la postura que asume el Tribunal Constitucional con base al artículo 18.4 CE, “no sólo pretende promover una acción legislativa y funcional de los poderes públicos para limitar el uso de la informática (aspecto pasivo), sino que quiere garantizar al ciudadano una esfera de poder autónomo que le permita decidir acerca del tratamiento automatizado de los datos que le conciernen, no sólo del nivel de conocimiento de su vida privada, sino el control de la información que le concierne y los usos que de ella se

³¹CONDE ORTIZ, Concepción, La protección de datos personales, un derecho autónomo con base en los conceptos de intimidad y privacidad, Dykinson, 2005, p. 29

³² STC, 11 -1998, de 13 de enero de 1998: FJ: 4 (RTC 1998/11)

puedan realizar.”³³ En este tema el autor señala también que no se trata de un derecho “semi gaseoso”, por el contrario, dice que es un auténtico derecho fundamental a una libertad positiva de control democrático, que sirve al ciudadano para defenderse de los posibles abusos del uso de la información personal tratada en los ficheros públicos o privados. De igual forma, nos hace una referencia sobre las alternativas o vías que puede usar el afectado; en este caso, se refiere al recurso de Habeas Data y los derechos instrumentales o garantías jurídicas subjetivas.

Ante estas circunstancias, debemos aceptar que nos sentimos más cerca de la interpretación que favorece la autonomía del derecho a la protección de datos, no sólo por aquellos datos que estén vinculados a la intimidad de la persona, sino todos en general. Creemos que la interpretación que hizo el Tribunal Constitucional, aunque implicaba riesgo, se hizo para hacer acorde el derecho con la realidad actual, que cada vez más tecnifica los medios de acceso a la información y que, de no haber tomado dicha determinación el Tribunal Constitucional, probablemente estaríamos frente a un desfase que en últimos casos causaría mayores inconvenientes a los afectados por la invasión a sus datos personales.

³³ OROSCO PARDO, Guillermo, “Protección de datos personales en el ámbito registral”, en ALVAREZ-SALA WALTHER, Juan, et al, Derecho de la empresa y protección de datos, Aranzadi, 2008, p.123

3.2. La Sentencia 292/2000³⁴ del Tribunal Constitucional Español: reconocimiento a la protección de datos como un derecho autónomo.

La sentencia 292/2000, dictada por el Tribunal Constitucional podríamos calificarla, muy respetuosamente, como “didáctica”, pues hace un análisis doctrinal extenso y más allá de destacar el parecido entre el derecho fundamental a la intimidad y el derecho fundamental a la libertad informática, llegó a establecer sus diferencias aspectos que han sido de extraordinaria relevancia para el posterior desarrollo de este derecho. En su redacción también hace una fuerte crítica e invalida la redacción original de algunos artículos de la LOPD 15/1999, en especial aquellos que permitían la sesión de datos entre Administraciones Públicas, sin el previo consentimiento de los titulares de la información.

A diferencia de las anteriores, es en esta sentencia en la que se logra diferenciar, con gran claridad, las características propias del derecho a la libertad informática³⁵, frente al

³⁴ La Sentencia 292/2000, surge a consecuencia del recurso de inconstitucionalidad que interpuso el Defensor del Pueblo, contra incisos de los arts. 21.1 (Comunicación de datos entre Administraciones Públicas) y 24.1 y 2 (Otras excepciones a los derechos de los afectados) de la LOPD 15/1999, por vulneración de los arts. 18.1 y 4 y 53.1 CE. En este recurso el Defensor del Pueblo señaló que tales artículos permitían, en primer lugar, hacer cesiones de datos entre Administraciones Públicas para fines distintos a los que motivaron su recogida. En segundo lugar, que el titular de esos datos no fuese informado, cuando se recaban, de la posibilidad de dicha cesión, al no estar prevista en la norma que crea y regula el fichero. En tercer lugar, que la propia cesión se efectúa sin el consentimiento del afectado. Y, en cuarto y último lugar, que la autorización para efectuar esas cesiones puede contenerse en una norma de rango inferior a la Ley. El Tribunal Constitucional señaló que efectivamente tales artículos adolecen de tal grado de indeterminación que deja excesivo campo de maniobra a la discrecionalidad administrativa, incompatible con las exigencias de la reserva legal en cuanto constituye una cesión en blanco del poder normativo que defrauda la reserva de ley.

³⁵ La libertad informática es el “derecho a la libertad” frente a las potenciales agresiones a la dignidad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos. Es un derecho a controlar el uso de los mismos datos insertos en un programa informático y comprende, entre otros aspectos, la oposición

derecho fundamental a la intimidad, pues “si bien comparten el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, se distingue del mismo porque atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la ley”. Según el Tribunal Constitucional, este derecho fundamental “comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros en los que han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes”³⁶.

Básicamente esta sentencia señaló que el derecho a proteger los datos no se refería necesariamente a los datos íntimos de la persona, sino a cualquier tipo de dato personal, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo el derecho a la intimidad individual, que ya estaría protegido por el artículo 18.1 de la Constitución, sino los datos de carácter personal en general. Además, que el consentimiento de las personas era imprescindible para usar su información, teniendo ellos siempre la facultad de actuar frente a los responsables de los ficheros.

Sobre lo anterior, entendemos que parte de lo que se pretende proteger no es sólo la intimidad de la persona, sino la apariencia que proyecta ante la sociedad o en todo caso, la opinión que otros puedan generar sobre el sujeto. En sí, conocer el nivel económico de alguien, con base a sus datos, puede hacerle candidato o no, a presiones externas para

del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

³⁶ STC, de 14 diciembre 2005, FJ: 2 (RJ 2006\968)

que se decante por uno u otro producto o servicio, en el peor de los casos, esa información serviría para excluir a la persona de ciertos beneficios concedidos a la sociedad, privarle de oportunidades laborales o inclusive colocarlo en marginación social.

Así, MURILLO DE LA CUEVA, señala que “el paso dado por la Sentencia 292/2000 es absolutamente inhabitual, no se ha dedicado a completar el régimen jurídico que para un derecho fundamental esboza la Constitución o a establecerlo para aquellos que se limita a mencionar sin dotarles de un determinado contenido”³⁷. El autor analiza cómo el Tribunal Constitucional reconoce un derecho que no está escrito en la Constitución Española, basándose en el artículo 18.4 de la CE y en instrumentos de Derecho Internacional, lo que, mediante una operación interpretativa compleja, le permite hallar un nuevo derecho y presentarlos con rasgos bien definidos. Sin embargo, matiza sus ideas al señalar que la tendencia de regulación a nivel internacional, en especial del Tribunal Europeo de Derechos Humanos, coincide en muchos aspectos con el criterio esbozado por el Alto Tribunal Español, todos en vía de reconocer el gran sentido y alcance de la protección de los datos personales.

A continuación, la STC 292/2000, reconoce y extrae del artículo 18.4 de la Constitución Española, un nuevo derecho fundamental, autónomo y lo diferencia del derecho fundamental a la intimidad, dando mayor independencia al principio establecido en el artículo 18.4 sobre libertad informática³⁸. Asimismo, restringió la posibilidad de la cesión de datos entre las Administraciones Públicas al ejercicio de las mismas competencias, o competencias que versen sobre las mismas materias, o al tratamiento posterior con fines históricos, estadísticos o científicos, siendo necesaria la autorización de las personas

³⁷ MURILLO DE LA CUEVA, Pablo Lucas, “Comentario al objeto (artículo 1 de la LOPD 15/1999)”, en TONCOSO REIGADA, Antonio (Dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas, 2010, p. 90

³⁸ El art. 18.4 CE fue esgrimido por primera vez en el caso de un ciudadano a quien el Gobierno Civil de Guipúzcoa le denegó información sobre los datos que poseía sobre su persona, resuelto por la STC, 254/1993, de 20 de julio.

afectadas por el uso de los datos incluidos en los ficheros, para que puedan cederse los mismos entre las Administraciones Públicas.

En esta sentencia, el Tribunal Constitucional, reconoce el amplio margen de cobertura de la protección de los datos, pues no solo incluye la información que sea estrictamente vinculada a la intimidad de la persona, sino que, además, protege todo el abanico de derechos que se incluyen dentro de los bienes de la personalidad³⁹. Aquí está claro que no todo dato puede tener la categoría de “intimo”, pero de todas maneras el derecho a la libertad informática, faculta a la persona a conocer y decidir sobre el uso que otros puedan dar a la información que le atañe. Del mismo modo, este derecho 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 indebida de los datos personales.

Este reconocimiento a la protección de datos, como derecho fundamental independiente, no ha sido fácil y quienes lo defienden sostienen que es necesario para lograr su justo lugar ante el conjunto de garantías constitucionales, porque de lo contrario, no existirían mecanismos jurídicos suficientes para su tutela, dada la insuficiente cobertura que posee el derecho a la intimidad para este tema y la diferencia que existe en la naturaleza de los derechos amenazados.

En síntesis, su nueva protección no podría considerarse como un impedimento a otros derechos, como es el caso de la libertad a la información y demás, pues si ese fuera el fundamento, también podría decirse lo mismo de la protección del medio ambiente, ante el derecho de producción y comercio. En este tema, GUICHOT dice que hay algunos datos que

³⁹ Los bienes de la personalidad son todos los derechos inherentes a la esfera personal del individuo. Solo tienen carácter personal y pertenecen a la sujeto por el solo hecho de ser persona, cuando adquieren la capacidad jurídica.

se vinculan más con otros derechos, y la intimidad no podría ser la única protagonista en este debate; por lo cual, pregunta ¿cabría entender que la protección de los datos sensibles (salud) sirve para garantizar el derecho a la vida privada, mientras que la del resto de los datos sirve a la protección de otros derechos o intereses?⁴⁰

Como respuesta reconoce que tal hipótesis es tentadora y más en el caso de la salud, pues indiscutiblemente se refieren al reducto tradicional de la intimidad, sin embargo, es evidente que no todos los datos guardan tan clara referencia y se vinculan más con otros derechos, como la libertad ideológica y religiosa. Sería tal vez cuestión de enfoque y señala que, en cualquier caso, no sería solamente el derecho a la intimidad en su sentido clásico sino, de forma más amplia, las posibilidades de libre desenvolvimiento en sociedad.

Consecuentemente, hay quienes piensan que la protección de los datos ya está suficientemente protegida mediante el derecho a la intimidad. HERRAN ORTÍZ señala que “el peligro (a la persona), no lo constituye un único dato personal aislado, sino el incesante almacenamiento y entrecruzamiento de la información personal, esto es, no representa gran amenaza que consten determinados datos personales, pero de todos es conocido que no existen hoy límites a la posibilidad de almacenamiento de datos, y que por el sólo hecho de ser registrados perjudican a la persona.”⁴¹

Sobre el particular, HERRAN ORTIZ, también se refiere a que una persona no sufre gran acecho a su intimidad, mediante la obtención de un dato aislado, que no pueda ser tratado o que no se vincule con otros del mismo titular, lo difícil o que preocupa es cuando la gran cantidad de datos acumulados de una persona se entremezclan y logran crear su perfil, capaz de mostrar su comportamiento, sus gustos, ideas, creencias etc., ante el público, sin

⁴⁰ GUICHOT, Emilio, Datos personales y Administración Pública, Thomson Civitas, 2005, p.37

⁴¹ HERRAN ORTIZ, Ana Isabel, El Derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos, Edit. Dykinson, 2002, pp.51 y 52

que esto haya sido consentido previamente por el afectado. Esta tesis también ha tenido sus detractores, cuando se habla de un concepto patrimonial de la protección de los datos personales, aquellos se niegan a aceptar el dominio absoluto de las personas de toda la información, porque estos temas deben estar excluidos de los bienes patrimoniales y pregonar su posesión sería restar a la sociedad de su derecho a estar informada.

PEREZ –LUÑO, ha señalado que la resistencia al reconocimiento de un derecho a la autodeterminación informativa autónomo, encuentra su justificación en el temor “a un concepto privatista del derecho, mediante el que se proceda a una indeseable identificación de este derecho como patrimonial, con la nefasta consecuencia de que en el supuesto de conflicto con otros derechos fundamentales éste quedaría abocado frecuentemente a la necesidad de ser sacrificado”⁴². Esta afirmación motiva nuestro razonamiento, pues hablar de conceptos de propiedad a veces trae aparejados otros derechos, como es el derecho comercial, no teniendo impedimento la posibilidad de “vender” aquello que sea nuestro. Sigo pensando en el desarrollo de las nuevas tecnologías, y reconozco que ahora existen nuevas figuras, como la venta de la información, negocio en el que las personas no ven obstáculos para vender sus datos, a cambio de otros beneficios. De hecho, ya existen empresas dedicadas a compilar información personal de usuarios y clientes, para después ofertarlas a otras entidades con el fin de ampliar las ventas de sus productos, ¿no sería esto una forma de posesión y posterior venta?

Y como no hay dos sin tres, otra crítica que se hace es que el derecho a la protección de los datos es meramente instrumental a otros derechos fundamentales, como el derecho a la dignidad o la intimidad. Sin embargo, no compartimos esta tesis, porque el mismo principio no operaría para derechos con clara “vocación instrumental”, como lo es el derecho a huelga, que surgen muy vinculados a la dignidad, pero igual tienen un

⁴² PEREZ – LUÑO, Antonio, “La libertad informática. nueva frontera de los derechos fundamentales”, en Libertad informática y leyes de protección de datos personales, Cuadernos y Debates, núm.21, 1989, p. 156

reconocimiento autónomo. Aquí, debemos decir que el carácter instrumental de algunos derechos no le quita su importancia; si esa fuese la intención principal, las constituciones estarían conformadas con uno o dos derechos y el resto serían meramente accesorios o instrumentales, lo cual podría ser una receta perfecta para el caos social.

En suma, desde una postura más filosófica, se ha criticado que hablar de derecho autónomo y fundamental no es lo más importante, porque la relevancia principal de un derecho no lo determina un legislador mediante un nombre, por el contrario, son los bienes que amparan dicho derechos los que determinan su valor y calidad ante los demás, si consideramos que el legislador no es quien construye y o crea a los derechos fundamentales (teoría iusnaturalista del derecho). Sobre el particular, no es nuestra intención establecer posturas sobre la naturaleza de los derechos fundamentales, ni entrar en el eterno conflicto entre iusnaturalistas e iuspositivistas, pero no podemos desconocer que persiste la incertidumbre con los datos, ya que cada vez se hace más difícil separarlos entre sí, y no se puede decir que la categoría no es importante, o que sólo es necesario atender un aspecto en concreto.

Siguiendo con la defensa de la protección de datos como derecho autónomo, también está la teoría de actualización del derecho fundamental, aunque de esta nos queda la duda, si este supuesto se ajustaría a la realidad social, si partimos de la base de que todos los derechos y más los fundamentales, surgen a consecuencia de las necesidades de las personas, y del momento histórico en el que viven, entonces, ¿el derecho a la intimidad surgió para protegernos del manejo de datos mediante los ordenadores?; parece que no, por el contrario, sí surgió para proteger a la persona y, poco a poco, ha ido ampliando su alcance, pero esto no significa que su núcleo conlleve la protección del tratamiento de los datos a este nivel tecnológico. Lo cierto es que existen características que dan trascendencia al tratamiento de datos y que convierten a la misma en especialmente sensible a los peligros derivados de la informática: su perdurabilidad, su carácter personal, que hace más complejo

el tipo de datos a considerar y en fin la diversidad de escenarios para los que pueden ser relevantes.

El derecho fundamental a la protección de datos no es ilimitado, al igual que el resto de los derechos fundamentales encuentra sus límites en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución. A su vez, esos límites o las restricciones directas que imponga el propio derecho fundamental pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho mismo.

Igualmente, algunos autores han señalado que el derecho a la autodeterminación informática y el derecho a la libertad informática, no son términos sinónimos y más bien persiguen objetivos diferentes. Contrario a esta posición, tal como señala HERRAN ORTIZ, “la libertad informática y el derecho a la autodeterminación informativa, pueden considerarse expresiones diferentes de un mismo objeto conceptual⁴³”, tesis que parece correcta y que esta investigación comparte sin reserva.

4. Normativa estatal sobre el derecho a la protección de datos personales.

Sobre este aspecto hay que señalar que tras la aprobación de la Constitución Española de 1978, en la que su artículo 18.4 ordenaba la existencia de una ley que desarrollara esta materia, no se aprobó la misma en un tiempo corto. Por el contrario, hubo que esperar 14 años para que se aprobara la primera ley encargada de regular los datos personales en España.

⁴³ HERRÁN ORTIZ, Ana Isabel, La violación de la intimidad en la protección de datos personales, Dykinson, 1999, p.80.

4.1. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LOARTAD).

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), desarrolló la orden aprobada en el artículo 18.4 de la Constitución Española de 1978 y por primera vez, se formalizó la limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, para garantizar la intimidad personal. En su Exposición de Motivos hace referencias al Convenio 108 del Consejo de Europa, pero en su texto sólo se refería a los datos tratados de forma automatizada, además que distinguía dos regímenes de regulación, uno encargado de los ficheros públicos y otro a los ficheros privados. Esta característica causó gran malestar pues se criticaba que generaba cierto nivel de preferencia para las entidades públicas, a la cual mantenía cierta amplitud de manejo, frente a una marcada severidad con que se regulaban los ficheros privados.

Mediante esta norma, se incorporaron al Derecho español los principios de calidad, del consentimiento del titular de la información, la protección de los datos sensibles, el deber de secreto de la información incluida en los ficheros y sobre todo los derechos ARCO (acceso, rectificación, cancelación y oposición) (Ver capítulo 5.2.), además que fue la norma por la cual se creó la Agencia de Protección de Datos. Sin embargo, no todo fue fácil en esta ley, también fue ampliamente criticada, pues no se emitía su reglamento, dejando un gran vacío sobre el alcance en la interpretación de algunos conceptos. Esta incertidumbre se solucionó casi siete (7) años después de la aprobación de la norma de 1992, siendo aprobado el Real Decreto 994/1999, de 11 de junio, por el cual se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal.

4.2. Ley Orgánica de Protección de Datos (LOPD) 15/1999, de 13 de diciembre, y su reglamento, el Real Decreto 1720/2007 de 21 de diciembre.

La LOPD 15/1999 que derogó la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, es la norma actual por la cual se protege la información de las personas.

Con esta nueva ley, se aprovecharon las experiencias logradas con su antecesora igualmente “se pretendía que los principios de protección de los datos de carácter personal, para el tratamiento de los mismos, que recogía la Ley Orgánica 5/1992, se ajustasen a los compromisos internacionales y a los principios constitucionales para la protección de los datos personales que puedan afectar al libre ejercicio de los derechos y libertades personales y, particularmente al derecho de la intimidad personal y familiar.”⁴⁴ Esta LOPD 15/1999 desarrolló los principios aprobados por la Directiva 95/46/CE, del PE y el CUE, de allí que tomó sus ventajas y también asumió algunos de sus vacíos.

Un elemento esencial que desarrolla esta ley es el concepto de dato personal, y los elementos que debe cumplir para poder ser amparado por la norma. Sin embargo, vale decir que, esta ley, a diferencia de la anterior, no se refiere únicamente a los datos automatizados, sino que incorpora a los datos tratados manualmente; pero no ampara a las personas jurídicas, siendo imprescindible que quien resulte afectado por el mal manejo de sus datos personales sea una persona física y que, además, sea titular de la información que ha sido incluida en el fichero. Es por esto que la Audiencia Provincial de Madrid señaló que “sea cual fuere la naturaleza de los datos recopilados, su incorporación a un sistema automatizado que permita su fácil manejo y su interconexión con otros es lícita a salvo de la

⁴⁴ ULL PONT, Eugenio, Derecho público de la informática protección de datos de carácter persona, Universidad Nacional de Educación a Distancia, 2003, p. 120

resolución que pueda dictar en cada caso la Agencia de Protección de Datos en el ejercicio de sus funciones...”⁴⁵

El tan ansiado reglamento a esta ley se concretó mediante el Real Decreto 1720/2007⁴⁶ de 21 de diciembre, que supuso también mucha ayuda para la interpretación de los términos usuales en materia de protección de datos. Este reglamento al igual que mencionamos con la LO 5/1992 se hizo esperar, pues desde varios años, ya existían dudas en torno a la interpretación de la LOPD 15/1999.

De este Real Decreto podemos decir que es muy positiva la forma como amplía las definiciones en su artículo 3, siendo más fácil de ubicar los conceptos en la mayoría de los casos. De esta forma, sale al paso de una crítica a la LOPD 15/1999 por su falta de organización en algunos temas.

Sobre lo anterior, no somos partidarios de la posición que mantiene, DAVARA RODRÍGUEZ, cuando señala que “esta metodología (definiciones), pone límites, de alguna forma a la más amplia interpretación y por tanto puede recortar el espíritu de la ley”⁴⁷. Sin embargo, este autor también señala como excepción el tema de protección de datos, por considerar que se trata de un área especializada. En particular, consideramos que mientras más clara sea la norma, especialmente con sus conceptos, mejor interpretación se hace de ella, ya que a veces por ser muy amplios en su uso, se pueden perder los objetivos de la propia ley.

⁴⁵ AAP de Madrid, 32-2002, de 11 enero, FJ: 1 (JUR 2002\95942)

⁴⁶ Publicado en el BOE, de 19 de enero de 2008.

⁴⁷ DAVARA RODRÍGUEZ, Miguel Á., La protección de datos personales en el sector de las telecomunicaciones, Universidad Pontificia de Comillas, 2000, pp. 13 y14

Ahora bien, este reglamento no escapa a críticas, y también se le señala que aunque en algunos aspectos su extensión ha sido clave para resolver temas pendientes de la ley, por otro lado, como en las facultades ARCO, que veremos más adelante, su extensión no logra resolver todas las dudas, quedando nuevamente en manos de la doctrina de la Agencia de Protección de Datos, y autoridades autonómicas, aquellos términos oscuros.

Punto y aparte, tal como lo habíamos señalados en las primeras páginas, elaborar una ley y su reglamento, llenos de intenciones, tratando de normalizar la actividad y la protección de los datos de las personas, no es la respuesta total al problema o por lo menos, su existencia no ha sido pacífica, pues aun queda hacer pública y de conocimiento general el contenido de dicha ley o reglamento. Esta difusión del derecho y de la manera para ejercitarlo tanto a nivel de la Agencia de Protección de Datos, como ante las autoridades locales o administrativas, ha sido lento, lo que trae consigo una desatención a la norma y la permanencia en el problema por el manejo de datos, entre ellos los expedientes clínicos, los cuales siguen apareciendo en contenedores de basura, sin la debida depuración de la información o custodia de los mismos.

La normativa vigente en materia de protección de datos obliga a cada entidad al cumplimiento de diferentes leyes, que a su vez implican mantener actualizada la información que poseen de los particulares, con independencia del nivel de seguridad de sus ficheros (Ver capítulo 5.5.4.), lo que trae consigo otro elemento difícil de concretar como es, entrelazar un aspecto tecnológico con un aspecto jurídico, a fin de lograr los objetivos propuestos por la norma. Esta nueva exigencia, unida al desconocimiento de empresas y usuarios de sus derechos y obligaciones, acrecentará algunos riesgos ya existentes, debido a la enorme cantidad de información “de sensible calidad” que ahora se encuentra digitalizada y a riesgo de ser intervenida por personas que no cuentan con la autorización del titular para su uso.

4.3. Excepciones a la LOPD 15/1999, de 13 de diciembre.

No todos los datos son objeto de protección por la LOPD 15/1999 esto no significa que los mismos estén desamparados o sin ninguna forma de controlar su acceso o dominio por parte de terceros. Para estos temas existen otras leyes como la Ley 1/1982 de 5 de mayo de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen; en su defecto aún queda la Ley Orgánica 2/1984, de 26 de marzo, que reglamenta el Derecho de Rectificación.

Aunque la norma aprobada para la protección de los datos ha sido diseñada para incorporar todos los medios posibles de protección ante la generación de ficheros y su posterior tratamiento, la misma ley también establece exenciones que podrían aplicarse bajo ciertos criterios. En este sentido, la LOPD 15/1999, en su artículo 2.2 señala que el régimen de protección de los datos de carácter personal no es de aplicación en los siguientes supuestos:

A. Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

B. Los ficheros sometidos a la normativa sobre protección de materias clasificadas.

C. Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

4.3.1. Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Esta excepción se refiere a los ficheros mantenidos por personas físicas cuyo propósito no es intercambiar información con terceras personas, no obtener un provecho más allá de la organización de la información que poseen para uso personal o doméstica. Tal es el caso de las agendas con datos de amistades de una familia o los registros que se hagan de las personas a quien acudir en caso de daños y reparaciones propias del hogar. Ahora bien, tal como señala la Audiencia Nacional⁴⁸, “en algunos casos lo personal y lo profesional aparece entremezclado. En este sentido el adverbio «exclusivamente» utilizado en el art. 2.2.a) apunta a que los ficheros mixtos, en los que se comparten datos personales y profesionales, quedarían incluidos en el ámbito de aplicación de la ley al no tener como finalidad exclusiva el uso personal”.

Conforme a la doctrina sentada por la Audiencia Nacional, existen algunos criterios que se deben atender, aunque la división es un tanto confusa y difusa, “uno, el criterio objetivo de la clase y la naturaleza de los datos tratados, según estén en conexión y se refieran a una esfera (la íntima y personal) o a otra (la profesional) de la actividad. Otro, el de la finalidad del tratamiento y circunstancias en que éste se desarrolla, criterio éste que operaría en aquellos casos en que alguno de los datos profesionales coincida con los particulares (por Ej. coincidencia de domicilio privado con el de la empresa, o cuando no se pueda acreditar si una deuda es de la empresa o si es personal del interesado)”⁴⁹.

Como ejemplo de lo anterior, y reiterando las diferencias, el Tribunal Supremo señaló que “es claro que los Arquitectos y Promotores a que se refiere el litigio participan de la naturaleza de personas físicas y que no dejan de serlo por su condición de profesionales o

⁴⁸ SAN, de 15 de junio de 2006, FJ: 3 (JUR 2006\195237)

⁴⁹ SAN, de 29 de marzo 2006 FJ: 3 (JUR 2006\144921)

agentes que intervienen en el mercado de la construcción, por lo que los datos personales relativos a los mismos, quedan amparados y sujetos en cuanto a su tratamiento informatizado a las previsiones de la LORTAD; y es que desde este punto de vista subjetivo la exclusión del ámbito de aplicación de la LORTAD no viene determinado por el carácter profesional o no del afectado o titular de los datos objeto de tratamiento, sino por la naturaleza de persona física o jurídica titular de los datos, en cuanto sólo las personas físicas se consideran titulares de los derechos a que se refiere el art. 18.4 de la Constitución”.⁵⁰

Además, esta misma sentencia amplía diciendo que “otra cuestión será determinar en cada caso y bajo el amparo y aplicación de la LORTAD, el carácter personal o no del dato de que se trate, que en este caso y como se ha indicado antes no puede ponerse en duda, pues se refiere al nombre, profesión, domicilio y demás circunstancias personales de los afectados, lo que es distinto de las relaciones sociales o profesionales que, según doctrina del Tribunal Constitucional invocada por la recurrente, no se comprenden en el derecho a la intimidad”

Está claro que, por ejemplo, un particular puede generar un fichero para compilar datos de sus amistades en su ordenador y así conocer toda la información que le parezca conveniente, con estricto uso familiar, lo que sin duda no queda sujeto al ámbito de aplicación de la ley. Sin embargo, en el caso médico, aunque el profesional no sirva a una empresa y realice práctica privada de su profesión desde su hogar, esto no significa que los ficheros que almacene son de carácter “familiar” y exento de cumplir la norma.

De lo anterior, lo más importante no es si existe o no tratamiento por parte de la persona, sino que su finalidad haya sido exclusivamente personal o doméstica y no se intente compartir la información con terceros.

⁵⁰ STS, de 20 de febrero 2007, FJ: 6 (RJ 2007\2790)

4.3.2. Los ficheros sometidos a la normativa sobre protección de materias clasificadas.

Para DÍAZ –PICAZO “en cualquier país que aspire a ser dueño de su propio destino, existen importantes informaciones cuya divulgación puede ser perjudicial para la entera colectividad”⁵¹. Esta afirmación encuentra sustento en la seguridad ciudadana, ya que es común que existan temas que, por su especial interés, deben ser tratados de forma separada y se le apliquen otras consideraciones que no impidan su seguro tratamiento. En este tema, el autor señala que, más que un debate sobre la existencia o no de este tipo de información, algo más importante es la regulación que se le da a los mismos, sin que esto riña con un propósito fundamental del Estado, como lo es la publicidad de la actuación de los poderes públicos.

Ahora bien, para tener mayor claridad en torno al presente concepto, es importante apoyarse en la Ley 48/1978 de 7 de octubre que modificó la Ley 9 de 1968, de 5 de abril, en su artículo único, señala que se entenderán como “materias clasificadas”, “los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimientos, por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado”.

Esta ley determina, además, que corresponde al Consejo de Ministros y las Juntas del Estado Mayor, la facultad exclusiva de determinar cuáles son las materias clasificadas. Además que toda la información obtenida será depositada en sitios reservados, cuyo acceso será controlado.

Sobre lo anterior, entendemos que aquellas materias que puedan afectar el buen orden del Estado, deben ser atendidas con prioridad y su contenido se reserve a pocos, dado los efectos que podrían provocar su difusión no controlada. Los programas de seguridad ahora son elaborados con mayor sigilo debido al alto nivel de expansión que tienen

⁵¹ DÍAZ –PICAZO, Luis María, Sobre secretos oficiales, Civitas, 1998, p. 37

las bandas criminales y a las posibles fugas de información que ponga en peligro a la población. Por ellos se permite que esta planificación tenga carácter reservado y sean unos pocos quienes tengan acceso libre a ésta.

4.3.3. Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

En cuanto al tercer supuesto, ya la Audiencia Provincial también ha dicho que “no puede negarse a la Administración Penitenciaria el establecimiento de mecanismos, contemplados en el ordenamiento jurídico, para hacer frente a cualquier eventualidad en el ejercicio de sus competencias, y es evidente la existencia de internos especialmente peligrosos y conflictivos cuyas interconexiones requieren la utilización de las técnicas informáticas modernas con el fin de contrarrestar la cada vez mayor organización de grupos de delincuentes con notorios intereses en el ámbito penitenciario”⁵²

Y es que en estos casos, la propia sentencia señala que “a diferencia de las relaciones de supremacía general, que unen normalmente al Estado con cualquier ciudadano, cuando la relación que une al administrado con la Administración es más intensa y especializada, con ciudadanos en una situación de sujeción especial (prestación del servicio militar, prestación de trabajo como funcionario público, o cumplimiento de penas en un centro penitenciario), la Administración titular del servicio público cuenta con poderes adicionales y, a su vez, el administrado (soldado, funcionario o interno en centro penitenciario) tiene obligaciones especiales.

Esto puede parecer ampliamente correcto si atendemos los graves delitos de terrorismo, en los que la falta de control y registro de los implicados en este tipo de delitos

⁵² AAP de Madrid, 32-2002, de 11 enero, FJ: 2 (JUR 2002\95942)

trae consecuencias tan duras con los ataques ejecutados el 11 de marzo de 2004, en la estación de Atocha en Madrid.

En cuanto a los Ficheros de Internos de Especial Seguimiento (FIES), por ejemplo, las normas para la realización de consultas médicas, tanto externas como internas, a los reclusos, establecen que se refuerzan las medidas de control, como es obvio conforme al tipo de condena que cumple cada interno, por lo que se le exige la autorización de la Subdirección General de Sanidad Penitenciaria, sin limitar los derechos de los internos a las normas de procedimiento. El propósito de estas normas es controlar el ritmo de salidas de los internos para consulta o ingreso en centros hospitalarios no penitenciarios, sin descuidar las garantías que el artículo 25.2 CE, establece para las personas privadas de libertad.

4.3.4. Los libros bautismales.

Sobre este tema, se han emitido múltiples sentencias, la mayoría de ellas con la intención de aclarar, si los ficheros que contienen los datos de una persona en los libros bautismales, están bajo la LOPD 15/1999, o por el contrario, no les es aplicable dicha normativa. En estas resoluciones judiciales se ha hecho todo un análisis para determinar si dichas anotaciones pueden ser consideradas un dato personal, si la acumulación de los mismos constituyen un tipo de archivo, y si la forma física o automatizada de los mismos permite, o no, el tratamiento de los datos, que en definitiva es lo que más está regulado en la LOPD 15/1999.

Todas estas causas parecen surgir con el interés de las personas de lograr la cancelación de dichos datos y evitar así su vinculación con una confesión religiosa en particular. En este aspecto, es motivo de interés para el derecho conocer si tales registros, efectivamente, pueden considerarse un tipo de “afiliación” con la religión en particular, o sólo se refieren al registro de un acontecimiento en la vida de la persona.

En este tema, PIÑAR MAÑAS dice que los libros bautismales no se pueden considerar como un fichero sometido a la LOPD 15/1999, “ya que dicha información no permite un acceso fácil a los datos que contienen y por tanto no pueden ser considerados un conjunto estructurado de datos”.⁵³ Entendemos que el autor haga referencia a que no cumplen con la sencillez en el tratamiento que establece la ley, para considerar al dato de carácter personal, y que estos libros bautismales generalmente se encuentran bajo sistema de archivo manuales, lo que hace muy difícil y desproporcionado su manejo por terceros, al estar regularmente aislados del resto de información personal. Pero esta característica de archivar manualmente los expedientes no se aplica en todos los casos, y no sorprende que en la actualidad existan también de forma automática, con apoyo de herramientas informáticas, situación que los haría más cercanos a la regulación impuesta en la LOPD 15/1999.

Lo anterior también trae como consecuencia la necesidad de analizar lo establecido por sentencias de algunos tribunales, como es el caso de la Audiencia Nacional⁵⁴, en la que señaló que “en primer lugar, ha de tratarse de datos de carácter personal y los que constan en el Libro de bautismo lo son, pues se concretan en el nombre y apellidos del bautizado, entre otros. En este sentido, el artículo 3.a) de la citada LOPD 15/1999, dispone que son datos de carácter personal “cualquier información concerniente a personas físicas identificadas o identificables”, y el nombre y apellidos, insistimos, lo son, pues revelan una información de identificación del titular de los datos, como esta Sala ha venido declarando con reiteración. En segundo lugar, deben estar registrados en un soporte físico, ya sea en soporte informático o no, y en el caso examinado constan en soporte papel. De manera que constituyan un fichero de datos, en los términos que posteriormente veremos. Y, en fin, en

⁵³ PIÑAR MAÑAS, José Luis, “Comentario al artículo 3 – concepto de dato de carácter personal”, en TRONCOSO REIGADA, Antonio (Dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas, 2010, p.187

⁵⁴ SAN, de 10 octubre 2007, FJ: 3 (JUR 2007\329400)

tercer lugar, este soporte físico ha de permitir su tratamiento o, mejor dicho, debemos estar ante datos “susceptibles de tratamiento”, ex artículo 2.1 ya citado. Teniendo en cuenta que el concepto de "tratamiento de datos personales" viene establecido en el artículo 3.c) de la LOPD 15/1999 como aquellas “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”, expandiendo el concepto previsto en la vieja Ley Orgánica 5/1002, de 29 de octubre, de regulación de Tratamiento Automatizado de Datos de Carácter Personal, que incluía únicamente el tratamiento automatizado”.

Sobre este tema, el Tribunal Supremo ha dicho que “los datos conservados en el libro de bautismo no hacen sino reflejar el hecho histórico de la realización de dicho bautismo en una fecha determinada y con respecto a una persona identificada, con los demás requisitos previstos en el Código de Derecho Canónico, en ningún caso como hemos dicho anteriormente, se configuran los libros de bautismo como una relación de católicos o personas pertenecientes a la religión católica y mucho menos como un fichero o relación actualizada de aquéllos por lo que carece de objeto pretender actuar sobre tales libros a efectos de hacer constar el abandono de la religión católica con el único objeto de actualizar una relación de miembros de dicha religión que no es tal.”⁵⁵ Surge la duda por la necesidad de inscribir en los libros bautismales la negativa de ciertas personas de mantener un registro en el que aparece que han cumplido un sacramento, en una determinada religión.

⁵⁵ ATS, de 21 abril 2009, FJ: 3 (JUR 2009\205870) Esta sentencia señaló además que en definitiva, los libros de bautismo, no tienen naturalmente la definición de recopilación de datos automatizados, sino manual, por lo que no responden al concepto de archivo estructurado según criterios específicos relativos a las personas.

4.3.5. Las personas jurídicas.

Los datos deben pertenecer a una persona física, a fin de que formen parte de la protección que establece la LOPD 15/1999. Pero esto no quita para que, mediante el Real Decreto Legislativo 1/2004, en su artículo 51, se proteja la información pertinente a las personas jurídicas, cuando señala que “tienen la consideración de datos protegidos el nombre, apellidos, razón social, código de identificación y domicilio de quienes figuren inscritos en el Catastro Inmobiliario como titulares, así como el valor catastral y los valores catastrales del suelo y, en su caso, de la construcción, de los bienes inmuebles individualizados”, en este caso, cuando las personas jurídicas sean titulares de bienes, se entenderá protegida la información en este aspecto.

4.3.6. Las personas fallecidas.

Tampoco se tienen bajo el amparo de la LOPD 15/1999, los datos pertenecientes a las personas fallecidas, en razón de que ésta sólo protege los datos de las personas físicas, en virtud del derecho a la personalidad, derechos que se pierden cuando la persona fallece. Pero, como indica el artículo 2.4 del Real Decreto 1720/2007, “las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos”. Este elemento de especial interés para los temas de salud, para aquellos casos en los que “el paciente”, pueda o no estar conforme a lo pretendido por la ley.

También en aquellos casos en los que el paciente conforme a su patología se mantiene asistido por aparatos, por ejemplo un ventilador mecánico, aunque sus constantes vitales reflejen que está vivo, no es menos cierto que su condición de autonomía está limitada a la existencia de una asistencia mecánica. En esto, no existe duda de que el

paciente está vivo y, en consecuencia, no podría utilizarse su información, pues a la luz del derecho se requiere del consentimiento de las personas responsables, el debate sería si su condición “es efectivamente” la que plantea la LOPD 15/1999 y su posterior reglamento. (Ver capítulo 5.2.5.)

Así en los casos del nasciturus, ¿se consideran protegidos por la norma?, si seguimos lo dispuesto por la Recomendación número R (97)5 de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa, en su artículo 4.5, dice que “los datos médicos relativos a niños no nacidos deben considerarse datos personales y gozar de una protección comparable a la de los datos médicos de un menor”. Aquí algunos autores han señalado que se refuerza su protección debido a que mediante ellos se puede conocer las características de sus progenitores, características que están basadas principalmente en perfiles de genéticos. (Ver capítulo 2.3.3.)

5. Identificación y configuración de los datos de carácter personal protegidos por la LOPD 15/1999.

5.1. La identificación del titular de los datos.

La identificación de la persona es el elemento más valioso a tomar en cuenta, frente a la calificación de la información. Por más que se pueda verificar si dicha información está automatizada o no, si es fácil o no ubicarla, lo más importante es si mediante ella se puede identificar a una persona física, pues como hemos señalado ampliamente, no se incluyen en este aspecto a las personas jurídicas.

Lo más evidente es proteger a la persona, por la posible afectación a sus derechos, por la compilación de su información, y los usos o beneficios que puedan obtener con ella. Si bien es cierto, al leer la LOPD 15/1999, está claro que no hizo una amplia

definición de este concepto, y en algunos casos aun nos queda apoyarnos en la luz que brinda la Directiva 95/46/CE, del PE y el CUE y más todavía el Real Decreto 1720/2007, para lo cual es importante poder conocer los tres tipos de personas señalados por la ley, que son, las personas identificadas, las personas identificables, y las personas anónimas.

De lo anterior, la persona identificada es aquella de la cual se conocen sus rasgos, que pueden ser físicos, sociales o de creencias religiosas. Entre los rasgos físicos, no sólo nos referimos a la forma física que tenga, sus rasgos étnicos o biométricos, sino también las características de su salud, elemento de suma importancia para la presente investigación. Y es que no es necesario que se conozca “toda” la información de la persona, basta con que sea suficiente para distinguirla del resto de los ciudadanos.

Por otro lado, la persona identificable, según nos dice el Real Decreto 1720/2007, en el artículo 5.1, apartado “o”, es toda “persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados”. Lo primero es resaltar que aquí, a diferencia del anterior, no se conoce quién es la persona dueña de la información, sin embargo mediante un esfuerzo regular y “no desproporcionado”, puede ser identificada.

Será entonces importante comentar que “el enlace” entre los datos y la persona se puede realizar mediante procesos, que regularmente son técnicos o automatizados, lo que en esta fecha se hace de simple ejecución, debido al gran avance de la tecnología y la cercanía con diversos recursos informáticos, lo que pone en evidencia lo fácil que es identificar al dueño del dato.

De esto, sería interesante conocer con exactitud a qué se refiere la ley con esfuerzo desproporcionado (Ver capítulo 2.4.1.), y partir de cuándo se puede decir que no es “fácil” su seguimiento, o por lo menos cuáles criterios determinan que un esfuerzo es extraordinario. Si bien es cierto, tanto el Real Decreto 1720/2007, como la Directiva 95/46/CE, del PE y el CUE no dan mayores detalles en este aspecto, lo que sí ha generado un cierto nivel de dudas. Por lo menos, la Recomendación No. R (97) 5 sobre protección de datos médicos (Feb. 13, 1997), elaborada por el Consejo de Europa, señala dos criterios interesantes para identificar qué es “desproporcionado”, tales son la cantidad de “tiempo” y “trabajo humano” requeridos, para saber si es o no identificable una persona.

Sobre los datos anónimos o de personas no identificadas (Ver capítulo 2.4.), la LOPD 15/1999 ha sido clara que no entran dentro de su cobertura, debido a que son datos que por su constitución, no permiten la identificación de una persona, lo que facilita su uso por parte de terceros⁵⁶. Sobre este aspecto, el Real Decreto 1720/2007 dice que se consideran datos disociados a “aquél que no permite la identificación de un afectado o interesado”. Para APARICIO SALOM, los datos disociados “son los datos personales que han dejado de serlo”⁵⁷ y es que, en resumen, tan pronto se aísla el dato, sin poder reconciliarlo con su titular, deja de representar una información sujeta a cobertura y protección de la LOPD 15/1999.

⁵⁶ La Directiva 95/46/CE, del PE y el CUE, define en su artículo 2, apartado f, al tercero como “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento”.

⁵⁷ APARICIO SALOM, Javier, Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Edit. Aranzadi, 2000, pp. 48 y 49.

5.2. El interesado o afectado.

El afectado o interesado es la persona física, titular de los datos que son utilizados para tratamiento. Este concepto fue definido por la LOPD 15/1999, en su artículo 3, apartado e y por el Real Decreto 1720/2007, en su artículo 5.1, apartado a.

Aunque parece simple y sin mayores dudas, a este concepto se le han formulado críticas, sobre su poca congruencia con otros ordenamientos jurídicos, como es el caso del Código Penal Español, que en su artículo 197.2 habla del “del titular de los datos o de un tercero”. Según HEREDERO HIGUERAS, aunque los términos se utilizan de manera indistinta, si existió intención por parte del legislador de utilizar una palabra que distinguiera ambos supuestos., ya que el concepto interesado es más propio de la legislación de Procedimiento Administrativo⁵⁸.

Sobre esto, todo titular de derecho, al verse involucrado en el uso de sus datos sin su consentimiento, podría considerarse como “afectado”, pero ¿todo afectado es titular de información? De ser así, entonces podrían incluirse en esta categoría a todas las personas que prueben algún nivel de afectación por parte de registro de los datos, sin ser dueñas de la misma. Tal aseveración desnaturalizaría la intención del legislador y dejaría vacío de contenido el concepto, que sólo busca dar la exclusividad a una persona.

Este principio parece incongruente con la filosofía descrita inicialmente por la LOPD 15/1999. Sin embargo, podría justificarse, a nuestro criterio, en aquellos casos de los menores de edad, sin capacidad de derecho, en el que la defensa se realiza mediante la representación de sus padres; asimismo, los casos de los fallecidos, en los que son los familiares quienes ejercitan los derechos de cancelación en nombre de su pariente.

⁵⁸ HEREDERO HIGUERAS, Manuel, La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, comentarios y textos, Edit. Tecnos, 1996, p. 76

En este último caso, recuerdo el comentario que hiciera HUALDE SÁNCHEZ en el que decía que “la defensa de la memoria del fallecido prevista en la Ley 1/1982 de 5 de mayo, no estaría encaminada a garantizar un residuo de los derechos de la personalidad, asegurando a título póstumo la defensa de la personalidad que no puede actuar por si misma, sino más bien la transmisión de un derecho de contenido patrimonial: la explotación comercial de los derechos de la persona fallecida o, si ello no es posible, la indemnización que en su caso pudiera corresponder”⁵⁹. Claro que en ese caso iba más referido a los derechos de la personalidad y de las facultades que tenían los parientes sobrevivientes, pero de una forma u otra, tal como lo hemos mencionado, en la LOPD 15/1999 también se reconoce derechos a los familiares de las personas fallecidas para la cancelación de datos de su pariente.

5.3. El responsable del fichero y el encargado del tratamiento.

El responsable del fichero y el encargado del fichero aunque podrían parecer lo mismo no lo son. De hecho, sobre esto ha existido un amplio debate⁶⁰, pues en la Directiva

⁵⁹ HUALDE SÁNCHEZ, José Javier, “La protección post mortem de los derechos de la personalidad y la defensa de la memoria del fallecido”, en ASOCIACIÓN DE PROFESORES DE DERECHO CIVIL, Bienes de la personalidad, Editum, 2008, p.100

⁶⁰ Según la SAN, de 16 de octubre de 2003, FJ: 2, (RJCA 2004\271). “No pueden existir dos responsables, uno del fichero y otro del tratamiento, porque fichero y tratamiento desde la óptica de la protección jurídica tiene una unión lógico-interpretativa. Como según la Ley el responsable del fichero o del tratamiento es el que decide sobre la finalidad, contenido y uso del tratamiento (no del fichero) es al concepto de tratamiento al que hay que acudir, sin que puedan existir independientemente un responsable del fichero y otro del tratamiento. En definitiva, y según resulta de las diez definiciones diferentes que figuran en el artículo 3 de la Ley de Protección de Datos, el responsable del fichero, o del tratamiento, es la persona que decide sobre el tratamiento, y la propia estructura y desarrollo jurídico-interpretativo de la teoría sobre protección de datos lleva a una sola solución. Esta misma sentencia, en su fundamento jurídico tercero, deja entrever que si existe tal diferencia entre responsable del fichero y responsable del tratamiento al señalar que “Se desprende asimismo de los

95/46/CE, del PE y el CUE sólo existe la figura de el responsable del tratamiento (definido en el artículo 2 apartado d.) no existiendo en ningún caso el responsable del fichero, dada la práctica diaria sí podrían existir diferencias entre el responsable del fichero y el encargado del mismo. Para conocer más detalladamente cada caso es necesario atender a lo dispuesto por la LOPD 15/1999, la cual señala en su artículo 3, apartados d y g, lo siguiente:

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

En el primer supuesto la LOPD 15/1999, conservó la terminología de la derogada LORTAD, y continúa con la denominación de “Responsable del Fichero”. En los casos de ficheros de titularidad pública, el responsable del fichero siempre será una Administración Pública, un órgano administrativo, o cualquier otro ente de derecho público, por su naturaleza.

repetidos apartados del art. 3, como ya se ha manifestado, la diferenciación de dos responsables en función de que el poder de decisión vaya dirigido al fichero o al propio tratamiento de datos. Así, el responsable del fichero es quien decide la creación del fichero y su aplicación, y también su finalidad, contenido y uso, es decir, quien tiene capacidad de decisión sobre la totalidad de los datos registrados en dicho fichero. El responsable del tratamiento, sin embargo, es el sujeto al que cabe imputar las decisiones sobre las concretas actividades de un determinado tratamiento de datos, esto es, sobre una aplicación específica. Se trataría de todos aquellos supuestos en los que el poder de decisión debe diferenciarse de la realización material de la actividad que integra el tratamiento. (el subrayado es nuestro)

La LOPD 15/1999, respecto de la anterior Ley 5/1992, de 29 de octubre de Regulación del Tratamiento de Datos de Carácter Personal (LORTAD) introduce importantes novedades. Una de ellas es la ampliación del régimen sancionador, dado que la LORTAD comprendía exclusivamente a los responsables de los ficheros (art. 42.1 de la LORTAD), y en la ley vigente comprende además a los encargados de los tratamientos (art. 43.1 de la LOPD), que según el art. 3d) de dicha ley es la persona física o jurídica, de naturaleza jurídica pública o privada, u órgano administrativo, que decide sobre la finalidad contenido y uso del tratamiento.

Esto encuentra su razón en que se pretende adaptar la legislación vigente a las exigencias de la Directiva 95/46/CE, del PE y el CUE, que tiene como objetivo dar respuesta legal al fenómeno reiterado de externalizar los servicios informáticos. En estos casos, de no existir tal ampliación, podrían actuar múltiples operadores, muchos de ellos insolventes, creados con el objetivo de buscar la impunidad o irresponsabilidad de los que le siguen en los eslabones siguientes de la cadena.

De igual forma, la disponibilidad o no del material por parte del responsable del tratamiento, no le exime de responsabilidad porque precisamente la LOPD viene a efectuar una ampliación subjetiva de este concepto, de manera que, por efecto de la externalización de los servicios informáticos, no queden impunes aquellos agentes que con capacidad de decisión sobre el tratamiento intervienen en el proceso, y aparentemente su actuación queda diluida por la relevancia de otras conductas más importantes en el proceso.

La figura del responsable del tratamiento se conecta así en la ley, con el poder de decisión sobre la finalidad, contenido y uso del tratamiento; poder de decisión que ha de diferenciarse de la realización material de actividades que integran el tratamiento, ya que será responsable tanto quién decida y trate como quien, teniendo el poder de decisión,

encomiende la materialidad del tratamiento a un tercero que actúe bajo la dependencia e instrucciones del primero.

De esta manera, a esta parte es a la que corresponde velar por la calidad del dato, que se recoge en el respectivo fichero. Especialmente debe garantizar que los datos son correctos, adecuados, pertinentes, no excesivos, y sobre todo deben estar al día. Aquí conviene recordar que todos los datos recogidos deben cumplir con lo establecido por la LOPD 15/199, en cuanto a la finalidad y la necesidad de existencia. En definitiva, el responsable del fichero “es quien decide sobre la creación del fichero, sobre su contenido y sobre su finalidad. En el caso de las administraciones públicas debe hacerse por medio de una disposición general”⁶¹.

A esta obligación concurren adicionalmente otras obligaciones, propias de su labor, como son el deber de secreto profesional (Ver capítulo 5.3.), GARRIGA DOMINGUEZ, explica que “el responsable del tratamiento o quien intervenga en alguna fase de éste se encuentra doblemente obligado al secreto cuando la información se refiera a la salud de las personas, ya que al deber establecido en la LOPD 15/1999, debe sumarse el regulado en el artículo 2.7 de la LOAP 41/2002”⁶². Por otra parte, el responsable del fichero deberá dar respuesta a los ciudadanos cuando éstos ejerciten ante el mismo sus derechos de acceso, rectificación, cancelación y oposición. Finalmente, también deberá adoptar medidas de seguridad, como el caso de la encriptación de información y la generación de normas básicas para controlar las consultas, que eviten el manejo de la información sin autorización adecuada, o en el peor de los casos se llegue a la alteración o pérdida.

⁶¹ LESMES SERRANO, Carlos, et al, La Ley de Protección de Datos análisis y comentario de su jurisprudencia, Lex Nova, 2008, p.108

⁶² GARRIGA DOMÍNGUEZ, Ana, Tratamientos de datos personales y derechos fundamentales, Dykinson, 2009, p.149

En esta calidad de responsable del fichero también se ubica a los centros sanitarios, pues con el fin de adelantar los servicios que prestan, generan los ficheros en los que quedan registrados los datos de sus pacientes, médicos colaboradores, funcionarios administrativos y demás datos necesarios para su normal funcionamiento. Claro está, que esta labor no la lleva a cabo una sola persona, más bien se realiza por un equipo entre los que conforman las autoridades de los centros sanitarios o propietarios en caso de centros particulares o privados.

Ante estas obligaciones, si el responsable del fichero no cumple con las mismas, puede ser sancionado, conforme lo establece la LOPD 15/1999, en este caso hay que aclarar que se le podrá imputar la comisión de alguna de las infracciones tipificadas en LOPD 15/1999. Si el responsable del fichero fuese parte de la Administración Pública del ámbito territorial de una comunidad autónoma que cuente con Agencia de Protección de Datos, será ésta agencia la encargada del trámite sancionador, pues posee dicha competencia.

Ahora bien, si el responsable es una empresa privada o una Administración Pública cuyo ámbito de competencia no está reglamentado de forma especial en una determinada comunidad autónoma, o bien la agencia especial de la comunidad autónoma no cuenta con el procedimiento sancionador será tramitado por la Agencia de Protección de Datos.

En el segundo supuesto, el artículo 3.g señala que el encargado del tratamiento puede ser una a persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Aunque es común que el responsable del fichero, puede igualmente ser el encargado del tratamiento, o sea, que no existirían diferencias en la persona en la que recaen ambas tareas, no es menos cierto que, en la práctica y de acuerdo a los modelos de gestión del servicio sanitario en los que se realice esta labor, puede que una misma “persona” no realice ambas tareas, pues una parte puede encargarse de tomar la decisión sobre el uso de los datos y la otra encargarse de gestionar lo decidido. Esta división implica que no solamente las tareas estén divididas, sino también las responsabilidades por cada tarea.

Por ejemplo una empresa capta la información de los particulares y establece un propósito y término de tiempo para su uso, sin embargo, por el volumen de trabajo requiere que otra empresa realice el análisis de los datos entregados por las personas y extraiga la información que espera obtener la empresa principal.

Se toma como ejemplo, los grandes hospitales que, en su labor de brindar una multiplicidad de servicios a sus clientes, compila para ello diversa información de los pacientes. Posteriormente, previo contrato con otras empresas, traslada los datos obtenidos para cumplir funciones médicas, de estadística, control de calidad, entre otros. En sí, la primera será la responsable de los ficheros por ser la que tiene autoridad para decidir la forma de captación, uso y vigencia de la información y la segunda será la responsable del tratamiento (análisis), por el término que dure el contrato, salvo que durante el mismo cambie sus obligaciones y decida sobre los datos, siendo en adelante responsable por el fichero, con sus correspondientes obligaciones.

5.4. Obligaciones del responsable del fichero.

La creación de un fichero, sujeto a las características que establece la LOPD 15/1999, trae como consecuencia la designación de un responsable del fichero y un

encargado del fichero. La propia legislación ha determinado que ambas figuras poseen, además de derechos, obligaciones frente al dueño de los datos. Estos derechos pueden ser reclamados no sólo por la vía administrativa, sino por la vía penal y civil.

En cuanto al responsable del fichero, el Real Decreto 1720/2007 no especifica “de forma expresa cuáles son los requisitos que habrá de cumplir este responsable de la seguridad, si bien los mismos se desprenden de sus propias funciones, ya que le corresponderá, como se ha indicado coordinar y controlar las medidas definidas en el documento de seguridad, analizando el contenido del informe de auditoría con el fin de proponer la adopción de las medidas pertinentes”⁶³.

Ahora bien, aunque existen múltiples áreas y todas muy importantes, debemos resaltar que en los temas de salud, por el alto impacto que pueden causar en las personas y quienes le rodean, no sería correcto que cualquier persona estuviese habilitada para llevar a cabo la recolección de este tipo de datos, puesto que “cabe entender que el tratamiento de los datos de salud está reservado a unos responsables cualificados”⁶⁴. Asimismo, como se verá en el capítulo 5.3. de esta investigación, aquellos que tengan acceso a la información están obligados a mantener en reserva cuanto hayan conocido y está prohibida su difusión a terceros.

Las Obligaciones del responsable del fichero son amplias, pero esta investigación tomará en consideración alguna de ellas, básicamente tomando la gran vinculación que tienen con el tema central de este trabajo, que corresponde a los datos de salud.

⁶³ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 1999, p.1

⁶⁴ HEREDERO HIGUERAS, Manuel, La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal, Tecnos, Madrid 1996, p. 104

5.4.1. Inscripción del fichero.

El deber más inmediato del responsable del fichero es cumplir con la obligación de inscripción del fichero, ante autoridad competente, que de acuerdo al tipo, privado o público, puede ser la Agencia de Protección de Datos Estatal o la Agencia de Protección de Datos de la comunidad autónoma correspondiente, según sea el caso. Ahora bien, esta obligación debe cumplirse después de haber realizado la publicación de su interés de constituir dicho fichero, en el Boletín Oficial del Estado o diario oficial correspondiente, esta obligación es previa a la constitución, modificación o supresión del fichero, por tanto, cualquier registro que se haga de los datos sin cumplir con ese requisito, no estaría amparado por la ley.

Según el Real Decreto 1720/2007, artículo 54, “La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

- a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.
- b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.
- c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.
- d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.
- e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

- f) Los órganos responsables del fichero.
- g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento”.

Este mismo artículo 54 señala que la disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los requisitos antes mencionado y de darse una supresión de los ficheros se debe establecer con claridad cuál será el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

Posterior a esto, corresponde al órgano competente de la Administración Responsable del fichero, para el caso de ficheros de titularidad pública, notificar a la Agencia de Protección de Datos o a la autoridad de control de una comunidad autónoma, cuando corresponde, dentro de los 30 días, contados a partir de la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

El artículo 55, apartado 2 del Real Decreto 1720/2007, señala que para los casos de ficheros de titularidad privada, igualmente deben ser notificada su creación ante la Agencia de Protección de Datos, específicamente por la persona o entidad privada que pretenda crearlos, teniendo en cuenta que ese también es un requisito previo a su creación. La notificación deberá indicar detalles imprescindibles, como son: la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en el que se

encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

Por otro lado, el Real Decreto 1720/2007 señala en su artículo 58 que la inscripción del fichero debe estar actualizada en todo momento, conforme el principio de actualidad del dato y cualquier modificación que afecte al contenido de la inscripción de un fichero tiene que ser previamente notificada a la Agencia de Protección de Datos o a las autoridades de control autonómicas competentes, para que éstos puedan proceder a su inscripción en el registro correspondiente. Ahora bien, si se decide eliminar o cancelar el fichero, igualmente debe comunicarse esta determinación ante la autoridad competente, a fin de registre la cancelación correspondiente.

De igual forma en el artículo 60 de este Real Decreto 1720/2007, se establece que es competencia del Director de la Agencia de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictar la resolución acordando, en su caso, la inscripción del fichero, sólo cuando se haya cumplido con el procedimiento respectivo. Con la inscripción, se establecerá un código único asignado por el Registro, las generales del responsable del fichero, la identificación del fichero o tratamiento, su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad que corresponde, según el tipo de dato que contenga el fichero.

También, en el artículo 62, el Real Decreto 1720/2007 señala que esta inscripción no está exenta de correcciones, por tanto, el Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones previamente aprobadas.

5.4.2. Informar y obtener el consentimiento del titular de los datos.

El deber de informar y obtener el consentimiento, se constituye en la piedra angular del tratamiento de la información, tanto es así, que en el caso del consentimiento, no puede existir dudas sobre su contenido y corresponde al Responsable del Fichero probar que posee la autorización del interesado para utilizar su información, “es precisamente el obligado a informar en los términos previstos en el artículo 5 de la LOPD 15/1999, quien debe acreditar el efectivo cumplimiento de su obligación”⁶⁵. Por esto, aunque “no puede exigirse para la obtención del consentimiento de los afectados, a la hora de tratar o ceder sus datos personales, que tal consentimiento se otorgue de forma escrita, pues no lo exige así ningún precepto de la ley, la entidad que pretenda obtener tal consentimiento deberá arbitrar los medios necesarios para que el mismo se preste de tal manera que no quepa ninguna duda de que efectivamente ha sido prestado, que la cesión de los datos ha sido consentida de modo tan clara que no pueda interpretarse en otro sentido”⁶⁶.

La información en la recogida de datos personales, también denominado principio de transparencia en el tratamiento de datos, constituye uno de los principios de la protección de datos, un derecho del afectado y un complemento previo de la prestación del consentimiento, “cuya omisión puede determinar un vicio del consentimiento para el posterior tratamiento de datos de carácter personal que origine la nulidad del mismo, siendo necesario para que el afectado pueda ejercer otros derechos que la LOPD le reconoce”⁶⁷. Esta obligación está presente en el artículo 5 de la LOPD 15/1999 y en el artículo 18 del Real Decreto 1720/2007.

⁶⁵ SAN, de 21 septiembre 2005, FJ: 4 (JUR 2005\262828)

⁶⁶ SAN, de 8 de octubre de 2008, FJ: 3 (JUR 2008\336710)

⁶⁷ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0340 – 2010, p. 2

Dado que existen múltiples opciones para recoger los datos, que van desde los formularios publicados en Internet, las llamadas telefónicas o la forma más tradicional (que consiste en la entrevista personal), es importante aceptar también que la acreditación de la efectiva información al afectado se puede realizar por diversos medios. No sólo mediante la aportación del documento firmado, sino que, además, se puedan aceptar la existencia de indicios que, de forma inequívoca, permitan probar que el interesado sí fue informado sobre el tratamiento de sus datos de carácter personal. De esta manera, es usual que en las páginas de Internet, se obligue al usuario a marcar la casilla de conocimiento de las políticas de privacidad de la página, antes de continuar con la entrega de los datos, y en las llamadas telefónicas se incorpore una grabación previa, en la que se advierta al usuario de los derechos que posee.

En igual medida, el derecho a información, realizado mediante notificaciones vía correo, han tenido diversas interpretaciones, por un lado, la poca certeza en el recibo y formalización de la comunicación y por otro lado, la falta de exigencia de la propia norma, de un procedimiento en especial. No obstante, tal como señala la Agencia de Protección de Datos, “podría resultar conveniente la utilización de medios fiables, independientes y auditables para la realización de las notificaciones o la obligación de comprobación de que los envíos no han sido devueltos por su destinatario”⁶⁸. Claro está, lo que hay que garantizar es que el dueño de los datos tenga conocimiento de sus derechos, siéndole comunicada tal situación por el responsable de fichero, pero eso en cierta medida, no parece estar totalmente acreditado, cuando se utiliza como medio de notificación el envío de una carta o misiva. (Ver capítulo 1.5.4.2.)

Por otro lado, en cuanto a la forma de comunicar estos derechos, la ley no establece un método en específico, más bien se refiere a las características de fondo, tampoco hace referencia, por ejemplo, al idioma que debe utilizarse, lo que podría causar

⁶⁸ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0020 - 2007, p. 2

cierta confusión en este aspecto. Bajo estos supuestos, consideramos que lo más recomendable es ser amplios, especialmente en la utilización de un lenguaje y una presentación fáciles de entender.

Por otro lado, si se trata de menores de edad, la obligación de información prevista en el artículo 5 de la LOPD exige un mayor rigor con el consentimiento, puesto que se dirige a una persona todavía no formada, lo que justifica que deba ser adaptada para que éste pueda comprenderla. En cuanto a la prueba del consentimiento de los menores, el artículo 12 del Reglamento 1720/2007 obliga que cuando se trata de menores de edad se establezcan mayores exigencias, para garantizar que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales. Cabe advertir que el artículo tampoco define un procedimiento en específico, quedando el responsable del fichero facultado de establecer aquellas que considere adecuadas. Aunque, como señala la Agencia de Protección de Datos, resulta aconsejable que además de la constancia de haber obtenido el consentimiento del menor y sus padres, “también se acompañe la fotocopia del DNI de los padres o tutores a fin de verificar que la firma coincide con la solicitud”⁶⁹ (de ser el caso). En este aspecto conviene ver el Capítulo 2.3.3. de esta investigación.

Lo anterior guarda relación, a nuestro parecer, con los objetivos que se quieren lograr al advertir al usuario sobre sus derechos, puesto que entregar información tampoco es un requisito fútil y no sólo se busca cumplir con una “imposición” legal. Más bien, lo que debe importar es que usuario comprenda “adecuadamente” el alcance de la entrega de su información, conozca que tiene derecho a no entregarla y que, si decide entregarla, aun le quedan derechos de control sobre la misma, así como sobre la identidad y dirección del responsable y sobre el uso que se va a dar a esos datos.

⁶⁹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico, 0046 – 2010, p. 3

Esta obligación de informar opera en todo momento, inclusive cuando corresponda a tratamientos de datos que realice la policía, en respuestas a las llamadas de auxilio que reciba de la población. En estos supuestos, la Agencia de Protección de Datos, sugiere que la Policía haga la advertencia de los extremos contenidos en el artículo 5.1 de la LOPD 15/1999 “al menos sucintamente, a través del establecimiento de una alocución permanente grabada en la que se haga referencia al tratamiento de los datos que se procede a realizar”⁷⁰. Según el artículo 45 del Reglamento de desarrollo de la LOPD 15/1999, ni siquiera en los casos de publicidad o prospección comercial se puede desconocer el derecho del interesado a ser informado, pues en estos supuestos, el responsable del fichero, además de comunicar los derechos que posee el interesado, también debe explicar de dónde obtuvo inicialmente los datos personales que posee; justificación que debe quedar reflejada en el documento de información sobre el tratamiento de datos que, en todo caso, si no se obtuvieron con el previo consentimiento del interesado, por lo menos, deben proceder de una fuente accesible al público.

En igual sentido, el empleador tendrá la obligación de informar al empleado de los derechos que le asisten antes de tratar sus datos, y, si fuese posible, hasta valdría incluir tales advertencias en el propio contrato de trabajo, de manera que no podría entenderse incumplido el deber de información, si el trabajador lee y acepta el contrato que se le propone, sobre todo porque la carga de la prueba siempre correrá a cargo del responsable del fichero. Aunque, para proceder posteriormente con su uso, no tenga necesidad de obtener su consentimiento; siempre y cuando se utilicen para articular la relación laboral y no se trate de datos de salud, pues estos últimos exceden del contenido que señala el artículo 5. Pues, si bien ha de informarse sobre el tratamiento, finalidades del mismo y destinatarios (cesiones previstas de datos), tal derecho no se constituye en un permiso abierto para tratar cualquier tipo de información. Sobre el primer supuesto, tiene su fundamento en que para la formalización del contrato de trabajo “existe un consentimiento

⁷⁰ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico, 0504 – 2009, p. 3

genérico del mismo por el trabajador respecto al uso de sus datos personales necesarios para el desenvolvimiento de dicha relación laboral, debiendo respetarse en la recogida de los mismos los principios que informan la protección de datos, recogidos en el artículo 4.1 de la LOPD.”⁷¹ Sobre los datos de salud del trabajador, se amplía en el capítulo 2.5.2.1.

El deber de informar, tal como hemos señalado en otros capítulos, es previo y no posterior al tratamiento de los datos, por lo que debe realizarse cuando el dato es recogido, sin que sea admisible pensar que es correcto omitir esta etapa o subsanarla posteriormente. Este deber no puede excluirse de las obligaciones del responsable del fichero y, de no hacerlo en momento oportuno, tendrá que cumplirlo posteriormente pese a los esfuerzos que eso represente. Así las cosas, si los datos no fueron recogidos directamente de los afectados, podría existir una excepción a este requisito, basado en el artículo 5.5 de la LOPD 15/1999. Pero, de no ser así, no será posible invocar “costos elevados” como excusa para no cumplir con este deber posteriormente.

Las obligaciones con el dueño de la información, es comunicarle de forma clara, expresa e inequívoca, los fines que busca con la recolección de los datos, así como obtener el consentimiento para cada finalidad, además, probar la existencia de dicho consentimiento, más cuando sea requerido por la autoridad. En esto es muy importante destacar que la obligación de probar la obtención del consentimiento, según reciente determinación, por ejemplo, no basta con una simple comunicación por correo (aunque este medio no sea exigido expresamente), más si el propio destinatario niega el conocimiento de tal misiva, aquí se dobla la obligación para el Responsable del Fichero, pues independientemente de enviar la carta, debe probar que se recibió oportunamente. En si, este criterio emitido por la Audiencia Nacional, aunque tiene validez, no permitió que la Agencia de Protección de Datos lo aplicará para casos anteriores a la emisión del criterio, pues a consideración del Tribunal, “en materia sancionadora, los nuevos criterios, por muy razonables que estos sean, ya estén

⁷¹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico, 0325 – 2009, p. 1

contenidos en una norma o deriven de una decisión de la Administración interpretando las normas, han de desplegar sus efectos hacia el futuro pero nunca proyectarse hacia actuaciones pasadas que se acomodaron a los criterios entonces existentes. La relación de los administrados con la Administración debe sustentarse en un principio de confianza legítima, confianza que sólo puede generarse cuando se tiene previsibilidad y seguridad en la actuación de la Administración”⁷².

En definitiva, el informe jurídico 0361/2010, destaca que ni el artículo 9 de la LOPD 15/1999 ni su Reglamento de desarrollo, imponen la utilización de medios técnicos concretos para conseguir dichas finalidades, dejando libertad a los responsables del tratamiento para elegir éstos siempre que se consiga el resultado previsto en dicho precepto⁷³. En consecuencia, si lo que se desea es pasar los documentos que contienen los consentimientos, de su versión física a electrónica, por ejemplo, no resulta exigible la utilización de una herramienta tecnológica determinada para la digitalización de los documentos, siempre que el responsable pueda garantizar la seguridad de los datos.

De todo lo anterior se reitera la Agencia al señalar que rige el principio de libertad de forma, tanto para la prueba de la obtención del consentimiento del interesado, como para la acreditación del cumplimiento del deber de información al mismo. No obstante, si se procede a la sustitución de los documentos originales en papel por un soporte informático, será preciso acreditar, en su caso, que en el proceso de automatización aquéllos no han sido alterados.

De esta manera, el artículo 9 de la LOPD 15/1999, impone obligaciones a ambas figuras en cuanto a la seguridad de los datos incluidos en los ficheros, siendo las siguientes:

⁷² SAN, de 19 octubre 2006, FJ: 8 (RJCA 2006\760)

⁷³ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico Nº 0361-2010, p. 2

1. Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No registrar datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Establecer, mediante reglamento, los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta ley (datos especialmente protegidos).

Sobre estas obligaciones hay que distinguir que se refieren a la relación que existirá, entre el Responsable/Encargado del Fichero, y los datos que registrarán, sin entrar a definir, las obligaciones que existirán entre ambas figuras, en el caso de que se trate de personas diferentes. Sobre este aspecto, los artículos 20, 21 y 22 del Real Decreto 1720/2007 desarrolla las condiciones de uso de la información, la posible subcontratación de los servicios y hasta la conservación de los datos contenidos en los ficheros. En si, dado que el responsable del fichero es quien decide sobre la finalidad, contenido y uso del tratamiento automatizado, y no quien le facilita el dato en virtud de un contrato celebrado con aquél, sólo él está sujeto al régimen sancionador establecida en la aludida ley, que no cabe extender a cualquier otra persona, pues, de hacerlo, se incurre en una aplicación extensiva o analógica del régimen sancionador, prohibida por el artículo 25.1 de la Constitución y 129.4 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento

Administrativo Común, con manifiesta conculcación de los principios de legalidad y tipicidad⁷⁴.

Ahora bien este derecho a exigir el consentimiento, se transforma a la vez en la obligación del responsable y encargado del fichero a mantener en secreto la información que posee sobre los usuarios del servicio de salud, secreto que para el Tribunal Supremo trata de salvaguardar o tutelar el derecho de las personas a mantener la privacidad de sus datos de carácter personal y, en definitiva, el poder de control o disposición sobre sus datos. Este deber de secreto está lógicamente relacionado con el secreto profesional.⁷⁵, en tal caso, el artículo 10 de la LOPD 15/1999 señala que están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. Esto cobra importancia dado que la LOAP 41/2002 señala en su artículo 5 que, la información no podrá entregarse a persona distinta a su titular, aunque se presente como familiar del mismo, mucho menos se podrá entregar información por vía telefónica, sin que se controlen las garantías mínimas para el titular de la información.

En particular, este tema fue analizado por la Agencia de Protección de Datos de la Comunidad Autónoma de Madrid, después de que se presentara queja contra el Hospital Infanta Sofía, en la cual una paciente denunciaba que su información personal había sido entregada a su ex marido, con antecedentes por malos tratos y orden de alejamiento⁷⁶. Del análisis del caso resultó la advertencia de la Agencia de Protección de Datos a las instituciones de salud, para que se verifique de forma exhaustiva, las generales de la persona

⁷⁴ STS, de 3 diciembre de 2002, FJ: 4 (RJ 2003\87)

⁷⁵ STS, de 10 junio 2011, FJ: 1 (RJ 2011\5195)

⁷⁶ Localizable en

http://www.madrid.org/cs/Satellite?c=PAPD_Generico_FA&cid=1142660358206&language=es&pageid=1247227049247&pagename=PortalAPDCM%2FPAPD_Generico_FA%2FPAPD_fichaResolucion&vest=1247227049247, fecha de la consulta 30 de enero de 2012, hora 11:20 a.m.

que consulta vía telefónica, antes de entregar información de salud. En si, se exige que el hospital, la Administración y el propio médico tomen todas las medidas de seguridad que sean adecuadas, y no entregar la información, a menos que se tenga rotunda certeza sobre la autenticidad de la persona titular de la información.

Estas medidas de seguridad no se exigen al azar, sino que están determinadas en el artículo 9 de la LOPD 15/1999 se establece la obligación de cumplir con la medidas técnicas y organizativas necesarias, que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. En este caso, no es recomendable entregar información sensible mediante comunicación telefónica, a menos que existan otros controles que debe verificar el responsable o el encargado del fichero, como podrían ser códigos o número de historia clínica que debe probar que conoce el interesado, antes de recibir algún tipo de información.

Del mismo modo, hay que aclarar que el concepto de entrega no implica el traspaso “físico” de documento alguno, pues, como hemos señalado anteriormente, la comunicación de la información no se limita a la entrega de algo tangible, sino que más bien obedece a la puesta en conociendo a otro de los datos de salud. Sobre el concepto de cesión que aparece en la LOPD 15/1999, MESSIA DE LA CERDA B., ha planteado lo importante que es distinguir entre el concepto jurídico tradicional que se da a la “cesión” y la aclaración que hace la propia LOPD 15/1999, con el concepto “comunicación”, dado que, en los casos de la información de salud, no es necesario entregar nada “físico”, como un fichero por ejemplo, como suele asociarse con el concepto “cesión”, sino más bien es la comunicación de los datos la que supone el peligro al derecho del enfermo, por tanto, “el mantenimiento del término cesión para referirse a las situaciones que aquí se analizan (LOPD 15/1999), supone un desacierto, solventado en gran medida por parte de la aparición del término

comunicación. La equiparación de los significados de ambas palabras elimina, al menos es parte, la impresión que supone la adopción de una terminología jurídica que posee un significado preciso y diferente del que se le atribuye en la legislación de protección de datos”⁷⁷.

Ahora bien, si se exige que la información previa al consentimiento, para los casos de mayores de edad, debe ser clara, es doblemente exigible para el responsable del fichero ser claro a la hora de recopilar datos de los menores de edad, pues esta condición implica que el lenguaje o los términos que se utilicen para advertir los propósitos del uso de los datos, debe estar en el rango de su leal saber y entender. En tal sentido, es al responsable del fichero y/o del tratamiento, como esta Sala también ha reiterado en numerosísimas ocasiones, a quien corresponde asegurarse de que aquél a quien solicita el consentimiento efectivamente lo da, y que esa persona que está dando el consentimiento es realmente el titular de esos datos personales, debiendo conservar la prueba del cumplimiento de la obligación a disposición de la Administración, encargada de velar por el cumplimiento de la ley⁷⁸.

Ahora bien, sobre los datos relativos a la minusvalía, la Agencia de Protección de Datos ha dejado claro algunos supuestos⁷⁹ en los que aplica excepcionalmente lo aprobado en el artículo 81.6 del Real Decreto 1720/2007, tales como:

1. La mera indicación del grado o porcentaje de minusvalía del afectado o de los miembros de su unidad familiar a los efectos previstos para el cálculo de las retenciones en la legislación reguladora del Impuesto sobre la Renta de las Personas Físicas.

⁷⁷ MESSIA DE LA CERDA BALLESTEROS, Jesús A. La cesión o comunicación de datos de carácter personal, Thomson, Madrid, 2003, p.42

⁷⁸ SAN, de 17 febrero de 2011, FJ: 2 (JUR 2011\77299)

⁷⁹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico, 0511 – 2009, p. 1

2. La indicación del datos “apto” o “no apto” de un trabajador a los efectos previstos en la Ley de Prevención de Riesgos Laborales.

3. Los datos relacionados con las obligaciones impuestas al empresario por la legislación vigente en materia de seguridad social que se limiten a señalar únicamente la existencia o no de enfermedad común, enfermedad profesional o accidente laboral o no laboral, así como la incapacidad laboral del trabajador.

Sobre el particular, señala que “lo único que se permite es adoptar medidas de seguridad de nivel básico en cuanto a dicho dato se encuentre afectado o vinculado al cumplimiento de deberes públicos, como sería el supuesto del fichero de nóminas en el que aparezca un porcentaje de minusvalía para calcular el nivel de retención aplicable en nómina, conforme a lo previsto en el artículo 103.1 del Real Decreto Legislativo 3/2004, de 5 de marzo por el que se aprueba el Texto Refundido del Impuesto sobre la Renta de las Personas Físicas”, e igualmente para casos en los que se deba conocer tal característica para conceder un derecho especial, como son las viviendas adaptadas para personas con discapacidad⁸⁰. De no ser así, si el dato de minusvalía se tratara para cuestiones que no constituyan el cumplimiento de deberes públicos, sí deberán de adaptarse medidas de seguridad de nivel alto⁸¹.

Después del análisis también se hizo excepción a la medida de seguridad alto, cuando el cumplimiento de la obligación no recae sobre el responsable del fichero, sino en el propio afectado, por ejemplo, en los casos de declaraciones fiscales, en los que es la persona la obligada a revelar su condición, por los motivos que imponga la ley, dicha situación permite al responsable del fichero establecer medidas de seguridad de tipo bajo, al amparo

⁸⁰ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0175 – 2010, p. 4

⁸¹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0008 - 2010, p. 3

del artículo 81.6. En informe jurídico se señala que “cuando los datos no se recogen para que el responsable cumpla con su deber legal sí son recabados con ocasión del cumplimiento por el propio afectado de dicha obligación, por lo que sí será posible entender que en el supuesto planteado, y siempre que los datos sean los meramente referidos a la discapacidad del afectado, operará la especialidad prevista en el artículo 81.6 del reglamento”⁸².

Los datos generales que se incluyen los ficheros académicos, no se consideran de nivel alto, más bien están ubicados en el nivel medio de seguridad, siempre y cuando no incluya ningún dato sobre el estado físico o mental del alumno. No obstante, “si el fichero contuviera datos referentes al perfil psicológico de los afectados y que hicieran referencia a la existencia de anomalías o especialidades de la personalidad del sujeto, habrá de considerarse que el fichero contiene datos relacionados con la salud de las personas, siendo entonces de aplicación lo dispuesto en el artículo 81.3 a) del reglamento, que exige la adopción sobre estos ficheros de las medidas de seguridad de nivel alto, además de las medidas de nivel básico y medio”⁸³.

Asimismo, se considerará merecedor de un sistema de seguridad alto, las pruebas y los resultados médicos, producto de tratamientos aplicados a los trabajadores⁸⁴ y, en igual medida, los datos relacionados a los resultados de las acciones de vigilancia de la salud en general, distintos del meramente referido a la aptitud del trabajador o que incorporan los datos relacionados con la patología que padece o accidente de trabajo sufrido por el trabajador, siendo responsable la empresa, por la protección de esta información, mientras estén bajo su poder.

⁸² AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0519 – 2009, p. 2

⁸³ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0572 – 2009, p. 2

⁸⁴ AGENCIA DE PROTECCIÓN DE DATOS, informe Jurídico 0623 – 2009, p. 3

Si se trata de ficheros automatizados, en los que el tratamiento se elabora fundamentalmente mediante el uso de ordenadores, entonces “el responsable del fichero deberá contar con las aplicaciones informáticas necesarias que permitan cumplir con las exigencias establecidas en el Reglamento de desarrollo de la LOPD 15/1999 en el que se recogen en la actualidad las medidas de seguridad a aplicar a ficheros y tratamientos...”⁸⁵. Tal exigencia no implica que toda la información contenida en esos ficheros deban tener uniformemente el mismo nivel de seguridad, es posible que se efectúe la segregación de los ficheros correspondientes, limitando las medidas de seguridad de nivel alto a aquellos ficheros que por la naturaleza de los datos que contienen requieren la adopción de este tipo de medidas, mientras que a los restantes se aplicarían aquéllas que, conforme a lo dispuesto en el artículo 81 del Reglamento, les correspondan.

Por otro lado, las ventajas que ofrece la tecnología en cuanto al uso de la información, también conlleva que el sistema informático dificulte no sólo copiar la información y trasladarla a un uso diferente, sino que también impida que personas no autorizadas puedan conocer, por vía de visualización, los datos de salud del paciente. Así, la Agencia de Protección de Datos ha advertido que “la visualización de los datos por personas diferentes al personal sanitario que pudieran encontrarse en la habitación del paciente cuando se accede a los datos, constituiría una cesión de datos definida en el artículo 3 de la LOPD 15/1999 como “toda revelación de datos realizada a una persona distinta del interesado.”⁸⁶

La LOPD 15/1999 establece las medidas de seguridad de nivel alto, con el fin adicional de disuadir que otros intenten obtener dicha información. Pero este objetivo no se lograría si no hay un serio compromiso por parte del Responsable del Fichero y sus representantes de establecer controles serios y adecuados a la información. En esto, la

⁸⁵ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0584 – 2009, p. 2

⁸⁶ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0501 – 2009, p. 2

Agencia de Protección de Datos insiste en que “la seguridad en el intercambio de información de carácter personal en la que hay que adoptar medidas de seguridad de nivel alto, en particular los requisitos de cifrado de datos, no es un tema baladí, ni un mero trámite administrativo, ni una cuestión de comodidad. Es el medio técnico por el cual se garantiza la protección de un derecho fundamental y al que hay que dedicar el tiempo y los recursos que sean necesarios para su correcta implementación.”⁸⁷

En cuanto a estos datos de salud, también hay que precisar algunos conceptos: es cierto que dichos datos son considerados como sensibles y merecedores de alta protección en la mayoría de los casos, pero esto no los convierte en “datos de nivel alto”, porque dicha característica no existe, su denominación correcta son “datos especialmente protegidos” y en consecuencia existen las “medidas de seguridad de nivel alto” que los protege. En ese sentido, “si bien normalmente ambos supuestos irán vinculados, es posible, en atención a las excepciones citadas, que el nivel pueda ser el básico con independencia de que los datos sigan siendo especialmente protegidos”⁸⁸.

Sobre el movimiento internacional de los datos, la LOPD 15/1999, también señala en su art. 33.2, su gran preocupación por prever que el sitio de destino tenga iguales medidas de control y protección sobre los datos personales. Recae esta gran responsabilidad en el director de la Agencia de Protección de datos, quien tiene que autorizar dichas transferencias, sólo en aquellos casos en los que existan dichas garantías mínimas.

5.4.3. El consentimiento del interesado en el uso de sus datos.

El principio del consentimiento informado en el derecho de protección de datos “representa una condición indispensable sobre la que se fundamenta la licitud del tratamiento

⁸⁷ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0494- 2009, p. 3

⁸⁸ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0382 – 2009, p. 3

de datos y su legitimidad”⁸⁹. Su razón es más que evidente, la autodeterminación del manejo de los datos, implica la posibilidad de las personas de decidir y la obligación del responsable de obtener la autorización debida antes de usar los datos de alguna persona. Este tipo de consentimiento no puede confundirse con el consentimiento informado para el tratamiento y diagnóstico de enfermedades, pues éste último corresponde a la autorización que otorgan los pacientes en el ámbito sanitario a los médicos durante su proceso de atención, debido a que “se orienta al modelo de responsabilidad o de la auto responsabilidad, que se asienta en una relación de horizontalidad o de igualdad en las relaciones entre médico y paciente”⁹⁰.

La LOPD 15/1999, en su artículo 6, señala que “el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa”, para lo cual, el Real Decreto 1720/2007, adiciona que “la solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.” Sobre el particular, ALMUZARA comenta el exceso de información que en ocasiones se solicita con respecto a un objetivo determinado. Un ejemplo podría ser los datos solicitados al interesado para el inicio de una relación contractual, en la que se recogen datos de identificación del cónyuge, edades de los hijos, gustos y preferencias, aficiones, etc.⁹¹

La correcta explicación que se haga sobre los objetivos que persigue el responsable del fichero condicionará que el titular de los datos autorice o no el uso de su información. Para HERRAN ORTÍZ, en alguna medida, la utilización de términos ambiguos,

⁸⁹ HERRAN ORTIZ, Isabel, El derecho a la protección de datos en la sociedad de la información, Op. Cit, p.57

⁹⁰ ALONSO ÁLAMO, Mercedes, “El Consentimiento informado del paciente en el tratamiento médico. Bases jurídicas e implicaciones penales”, en MENDOZA BUERGO, Blanca (editora), Autonomía personal y decisiones médicas, Thomson Civitas, 2010, p.98

⁹¹ ALMUZARA ALMAIDA, Cristina, “Relaciones pre contractuales y contractuales”, en ALMUZARA ALMAIDA, Cristina, Estudio práctico sobre la protección de datos de carácter personal, Lex Nova, p.105

tanto en la Directiva 95/46CE, como en la redacción de la LOPD 15/1999, puede causar variadas interpretaciones en cuanto a la aplicación de los principios protectores de la información de los ciudadanos. Sin embargo esto no excluye ya que exista un binomio directo entre la obligación de obtener el consentimiento y la obligación de informar previamente al interesado.

Sobre el consentimiento, señala GUICHOT que se ha planteado si el consentimiento al que se refiere la LOPD 15/1999 puede ser tácito o necesariamente debe ser expreso, a lo que la Agencia de Protección de Datos señala que “la exigencia de consentimiento inequívoco 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”⁹². De lo anterior hay que matizar y señalar que el consentimiento tiene que ser expreso en aquellos casos en los que se traten datos de carácter sensibles; ejemplo, la salud.

Por otro lado, para el resto de datos, basta con que el responsable del fichero conceda al interesado un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. Aunque, en este tema, dice el autor, resulta por demás polémico, pues supone de facto desplazar una carga, la de oposición, a los afectados, que en muchas ocasiones por comodidad o por ignorancia no realizarán ninguna conducta, permitiéndose de este modo el tratamiento de la información de forma más relajada.

Evidentemente, informar requerirá un nivel de esfuerzo que la ley exigirá cumplir al responsable del fichero, situación que no siempre es la misma, pues en aquellos casos en los que el esfuerzo resulte excesivo o imposible, a criterio de la Agencia de Protección de

⁹² GUICHOT, Emilio, Datos personales y Administración Pública, Op. Cit, p237

Datos o del organismo de protección de datos equivalentes (conforme a la cantidad de personas, la antigüedad de los datos y a las posibles medidas compensatorias), se podrá exceptuar de este requisito, según se establece en el artículo 5, apartado 5 de la LOPD 15/1999.

De lo anterior, han surgido algunas críticas. Por ejemplo, para RODRÍGUEZ ESCANCIANO, esta opción no contempla las realidades laborales, ya que en aquellos casos en los que resulte difícil comunicar individualmente, bien podría sustituirse dicha situación por información a los representantes unitarios o sindicales de los trabajadores. La autora señala el olvido de la norma y de la excepción, a los aspectos laborales que se ven involucrados en la protección de datos⁹³.

En relación con esto, quedan algunas dudas sobre si la comunicación al representante sindical es suficiente para cumplir con los criterios protectores de la LOPD 15/1999, y es adecuado como para aceptar que se ha cumplido con una notificación individual. De acuerdo a esta investigación, parece que los representantes sindicales sí podrían ayudar a realizar la notificación o poner sus medios a disposición para que tal objetivo se cumpla, pero esta acción no podría reemplazar totalmente el derecho que tiene cada individuo sobre sus datos personales.

Este tipo de consentimiento no está limitado al tipo de participación que tenga una persona en los objetivos que busca alcanzar el Responsable del Fichero, inclusive aunque "la participación sea en un programa, en el que va a ser observado a través de las cámaras de televisión por millones de espectadores, no se puede "despojar" totalmente a un ciudadano de su derecho a la intimidad, porque su libertad sigue intacta y conserva el pleno derecho a

⁹³ RODRÍGUEZ ESCANCIANO, Susana, El derecho a la protección de datos personales de los trabajadores nuevas perspectivas, Bomarzo, 2009, p. 28

que nadie trate, ceda o revele sus datos personales, aunque voluntariamente el mismo los haya facilitado para concursar".⁹⁴

Esta autorización no se limita a un único acto, pues de existir varios propósitos para la información que se pretende recabar, de no solicitarse los permisos en un primer acto, deberá solicitarse con cada objetivo diferente que se utilice. Así, el Tribunal Supremo ha señalado que "dicha obligación existe en relación con todos los datos de carácter personal que se solicitan de su titular y que vayan a ser objeto de tratamiento, de tal forma que si se producen distintas solicitudes sucesivas en el tiempo, el titular debe tener conocimiento que todas ellas tienen como destino su tratamiento..."⁹⁵. Asimismo, el Tribunal Supremo ha recalcado que la finalidad que persigue la obtención de los datos se constituye en un elemento fundamental para definir la existencia o no de consentimiento por parte del afectado. Así, en una sentencia de la Audiencia Nacional, en un caso sobre cesión de datos entre empresas, señaló que "esa cesión de datos, dado que se refería a una finalidad totalmente ajena al contrato de suministro eléctrico que los clientes tenían suscrito con ..., y que ni siquiera de forma tangencial se mencionaba en la carta que recibieron sobre nuevos servicios de entidades del grupo a que aquella pertenecía, requería, en aplicación de esa LOPD, el consentimiento inequívoco de los afectados..."⁹⁶.

5.4.4. El deber de secreto.

El secreto, en cuanto a la protección de los datos, recae sobre el Responsable del Fichero y todos aquellos que, en el ejercicio de sus funciones, tengan acceso a los datos de una persona. Esta obligación es impuesta por la ley a los custodios de la información, precisamente por el tipo de actividades que realizan. "El referido deber de sigilo o discreción

⁹⁴ SAN, de 31 enero 2003, FJ: 3 (JUR 2005\190525)

⁹⁵ STS, de 17 abril 2007, FJ: 6 (RJ 2007\3295)

⁹⁶ SAN, de 22 junio de 2005, FJ: 7 (RJCA 2005\924)

también recae lógicamente, sobre el responsable y el encargado de los ficheros automatizados cuando la información corresponde a persona, con derecho a exigir que dicha información se mantenga en reserva, en forma adecuada⁹⁷. Además, aunque parecido, no es el mismo deber que guardan los médicos para el caso de los datos de salud (ver capítulo 5.3.), dado que aquél es un tipo de secreto diferente, clasificado como secreto profesional⁹⁸, cuyas características ampliamos en otra parte de esta investigación.

Aun se debate sobre cuál es el núcleo del secreto que debe guardar el responsable del fichero y el responsable del tratamiento, si es la información per se, o el deseo o ánimo de callar. En esa medida, hablar de secreto del dato podría tener dos interpretaciones o significados: por un lado, está la información, propiamente tal, que se desea proteger de terceros; y por otro lado, está el estado mental o comportamiento de quienes poseen dicha información, lo que se manifiesta en su propia manera de actuar.

Por todo lo anterior, no es de sorprender que el Responsable del Fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo⁹⁹. Aquí, se hace alusión a los contratos de servicios que podría constituir el responsable del fichero con terceros (encargados del

⁹⁷ MORALES PRATS, Fermín, "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en QUINTERO OLIVARES, Gonzalo (Dir.), Comentarios a la Parte Especial del Derecho Penal, 5 edición, Edit. Aranzadi, 2008, Navarra, p. 445

⁹⁸ Dependiendo del tipo de información que se posee y de las partes intervinientes, hay quienes distinguen entre el secreto profesional (del médico, periodista, abogado, entre otros), el secreto comercial (también llamado secreto de empresa o de fábrica), Secretos a los que están obligadas las autoridades y los secretos de Estado.

⁹⁹ SAN, de 9 noviembre 2005, FJ: 4 (JUR 2006\122198)

tratamiento) y que tienen efectos no solo durante la tenencia de los documentos, sino más allá de finalizar el contrato.

Como quiera que estos datos no se comparten con todos y el desconocimiento generalizado de información hace que su adquisición sea más difícil, se obliga al Responsable del Fichero y demás personas involucradas a establecer mecanismos que hagan que este proceso sea muy formal y bajo controles permanentes, su obtención ilegal sea muy complicada o costosa y que, de no existir el consentimiento del titular, se pueda rechazar cualquier intento de ingreso ilegal al fichero.

La LOPD 15/ 1999 establece en estos supuestos tres tipos de infracciones, y las califica como leve, grave y muy grave, con lo cual puede imponer multas a quienes no guarden el debido secreto de la información. Este tipo de infracciones las califica así:

En el artículo 44.2e, señala como infracción leve el incumplir el deber de secreto establecido en el artículo 10 de la propia LOPD 15/1999, salvo que constituya infracción grave. Este tipo de falta podría acarrear multas que oscilan entre 600 a 60,000 euros.

Asimismo, en el artículo 44.3.g señala como infracción grave la vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo. Este tipo de falta podría acarrear multas que oscilan entre 60, 000 a 300,000 euros.

Por otro lado, el artículo 44.4g, tipifica como infracción muy grave la vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los

apartados 2 y 3 del artículo 7 de la LOPD 15/1999 (entre los cuales están los datos de salud), así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas. Este tipo de falta podría acarrear multas que oscilan entre 300,000 a 600,000 euros.

El elevado monto de las multas es una forma muy directa de invitar a los Responsables del Fichero a mantener un estricto control sobre la información que poseen, establecer adecuadamente los criterios de seguridad y generar cuanto contrato sea necesario, si decide ceder información, a fin de promover el tratamiento de los datos.

5.4.5. Establecer las medidas de seguridad.

Acopiar datos tiene como consecuencia lógica el establecimiento de medidas de seguridad para protegerlos. Básicamente, el propósito de estas medidas es “impedir el acceso a los sistemas de datos personales en particular y a los datos en general, a personas no autorizadas, o para evitar el desvío de la información, malintencionadamente o no, hacia sitios no previstos, además de garantizar el tratamiento de datos dentro de los límites permitidos por la norma y con respeto a los derechos del interesado, asegurando la confidencialidad y la integridad de los datos personales evitando su alteración, pérdida, transmisión y acceso no autorizado”¹⁰⁰. De igual forma, la normativa vigente en materia de protección de datos establece un conjunto de medidas de seguridad “cuyo objetivo no es impedir, en el caso de los ficheros públicos, el acceso a los datos por parte de empleados públicos determinados, sino establecer una limitación de acceso a los datos con carácter general, permitiéndolo exclusivamente a aquéllos empleados públicos que para el ejercicio de sus funciones precisen tener conocimiento de datos en ellos contenidos”¹⁰¹.

¹⁰⁰ DAVARA FERNÁNDEZ DE MARCOS, Isabel, Hacia la estandarización de la protección de datos personales, La Ley, 2011, p. 360

¹⁰¹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0183 – 2009, p.1

El artículo 9 de la LOPD 15/1999 impone una obligación especial al Responsable del Fichero y ésta es la de adoptar medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. El legislador ve necesaria la imposición de tales medidas, con base en el desarrollo de las tecnologías y el riesgo que esto supone para la información de las personas, pero tampoco deja de mencionar que estos riesgos no están sujetos solamente a la voluntad humana, sino que también en ocasiones se puede deber a riesgos que provienen del medio físico o natural.

Por tanto, para cumplir con los términos de seguridad es necesario limitar el acceso y permitir sólo a quien esté autorizado. En este caso, un usuario que, en los términos de la consulta, es la persona física que accede al fichero. Asimismo, concretar su perfil mediante el cual se puede definir el tipo de información a la que éste puede acceder y el tipo de acciones que puede realizar. No obstante, la idea de establecer usuarios únicos impide que existan usuarios y contraseñas compartidas, para lo cual es necesario que cada usuario tenga un código de carácter exclusivo y que, a la vez, sea secreto. Por ello, debe implantarse un procedimiento que garantice la seguridad y confidencialidad en el otorgamiento de identificación y autenticación de los usuarios (esto es, que la contraseña sólo sea conocida por el usuario). De igual forma, este requisito de individualización debe cumplirse para todos los usuarios que accederán a los ficheros, aunque éstos tengan el nivel básico, a diferencia de la normativa anterior (LOARTAD) en la que tenían cabida los usuarios genéricos.

El problema de las claves compartidas, además de la propia inseguridad en la conservación de los datos, es que no permite determinar con claridad la identidad de los que utilizan la misma clave de un usuario en un momento determinado, lo que impide saber si el acceso a los datos estaba debidamente autorizado y si los usos posteriores a este acceso son compatibles con la finalidad para los que fueron recabados. De darse una cesión, no se

podría establecer quiénes son los responsables por no cumplir con los criterios básicos, que en esta materia tiene reglamentado el Real Decreto 1720/2007. De esta forma, “la utilización de claves de acceso, que permitan al interesado tener conocimiento en cada momento de los datos de carácter personal existentes en el fichero resulta sumamente útil, siempre y cuando dicha clave o “dato de control” asegure el carácter personalísimo de la consulta efectuada para conocer la situación concreta a la que se acceda”¹⁰².

Los ingresos al fichero cobran más rigurosidad conforme al tipo de nivel de seguridad que se establezca. En los niveles de seguridad básico, existirá como mínimo, una contraseña para poder acceder a la información; en el nivel medio, esta medida de identificación y autenticación se vuelve más rigurosa ya que, a las medidas anteriores previstas para el nivel básico, se añade la obligación de establecer un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información (art. 98); y en el nivel alto, no basta con imponer códigos, ni limitar los intentos, además, un registro de cada intento de acceso que se produzca, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado (art. 103).

Esta obligación de establecer medidas de seguridad para los ficheros se contempla en diversos ámbitos. El art. 12.2 de la LOPD 15/1999 señala la obligatoriedad de establecer esta protección para los datos, sobre todo, en casos de cesiones de la información. Aquí las medidas de seguridad se contemplan como parte integral de contrato y el propósito de la reglamentación en esta materia es no dejar al libre albedrío de las partes la protección de los ficheros.

Del mismo modo, estas medidas de seguridad se encuentran entre los requisitos básicos que se deben aportar para poder inscribir un fichero de titularidad pública o privada

¹⁰² AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0021 – 2009, p. 5

(art. 20,2 h y 26,2) y, además, a ambos se les exige que hagan alusión al nivel de estas medidas, entre las que se encuentran los nivel bajos, medios o altos. Aún así, “debe recordarse, además, que, tal y como se observa en dicho precepto, las medidas de seguridad tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores¹⁰³”.

Las medidas de seguridad serán aplicadas conforme al tipo de fichero a que corresponda y de la finalidad a que esté vinculado el fichero o el tratamiento. El Real Decreto 1720/2007, que reglamenta la LOPD 15/1999, en su artículo 80 las clasifica de forma general en tres tipos, de nivel básico, medio y alto.

En el caso de los datos de salud (ver cap. 4), el artículo 81.3.a establece que la seguridad debe ser tipo alto, aunque por vía de excepción a esta exigencia general, dispone en su artículo 81.6 que se pueden establecer medidas de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

5.5. Principios en la protección de datos de salud.

Al igual que el consentimiento, también es importante mantener otras exigencias esenciales para garantizar una adecuada recolección del dato y ajustar su gestión a un proceso limpio y conforme a derecho, antes y durante el proceso de su tratamiento. La Directiva 95/46/CE, del PE y el CUE así lo contempla desde su redacción inspirada en el derecho de las personas. Así, el artículo 4¹⁰⁴ de la LOPD 15/1999 y el artículo 8 del Real

¹⁰³ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0410-2010, p.3

¹⁰⁴ Artículo 4 de la LOPD 15/1999

Decreto 1720/2007, han reglamentado esta materia, dentro del cual se destacan los siguientes principios que se detallan a continuación.

Los principios generales que definen la calidad de los datos se pueden considerar a su vez, como las pautas mínimas a las que debe atenerse la recogida, tratamiento y uso de datos de carácter personal, principios encaminados a garantizar tanto la certeza de la información contenida en los datos almacenados cuanto la congruencia y racionalidad de la utilización de los mismos. Estos principios se nutren del derecho fundamental a la protección de los datos, reconocido en el artículo 18.4 de la CE, bajo la referencia al uso de la informática, y que extiende su protección no sólo a los datos íntimos de la persona, que ya

-
1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
 2. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
 3. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
 4. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
 5. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
 6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
 7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

poseen cobertura jurídica mediante el derecho a la intimidad y que en todo caso gozan de protección reforzada en el LOPD 15/1999, sino también a los datos de carácter personal.

5.5.1. Principio de lealtad.

El principio de lealtad es ante todo una obligación para quien solicita la información, y toma su fundamento en la prohibición de engañar a las personas y evitar que sufran daños a su patrimonio o su moral. Es indiscutible que “engañoso y fraudulento” son términos sustancialmente equivalentes¹⁰⁵ y por ese tipo de conducta es que se reitera la necesidad de mantener el principio de legalidad como obligatorio, ya que puede considerarse como la fuente de la que toman fundamento el resto de principios destacados en la norma, ya que muchos de ellos se basan en el comportamiento del responsable del fichero, de forma tal que, si no existe lealtad y legalidad en el mismo, difícilmente se puede cumplir con los otros.

Este principio es de extraordinaria validez para el tratamiento de los datos, porque representa la columna vertebral del resto de principios. De poco sirve obtener el consentimiento de una persona si se logra con base a mentiras, o peor, que se brinde información previo a la recolección de los datos, pero dicha información sea incorrecta. En esto, el Real Decreto 1720/2007, no se define aun con claridad cuáles son los contornos que se ajustan a una conducta leal o no leal, lo que provoca que se eche en falta una definición más precisa en este aspecto.

Siguiendo a EGUSQUIZA BALMASEDA, “esta falta de determinación normativa sobre las acciones que se entienden leales en el tratamiento de los datos, permite que puedan corregirse conductas inicialmente lícitas que, sin embargo, pueden minar el derecho

¹⁰⁵ STS, de 27 mayo 2011, FJ: 3 (RJ 2011\4803)

a la intimidad del paciente”.¹⁰⁶ Tal parece que dicha ausencia puede reducir el nivel de protección que se exige para los datos personales en general, lo que se traduce en mayor riesgo del paciente, por ejemplo, ante un probable abuso de su información y abre la puerta para que posibles estrategias tendentes al engaño puedan realizarse.

5.5.2. Principio de proporcionalidad.

De manera general, debe entenderse que este principio busca proteger a las personas sobre la “cantidad” de información que puede pedir el Responsable del Fichero, para así lograr el fin determinado. Usualmente estos extremos son fáciles de definir, aunque no es una regla permanente para todos los casos, ya que la cantidad de datos a recolectar suele estar determinada por el fin que se persiga.

Así, por ejemplo, si se pide información para formalizar la reserva de una habitación de hotel, lo más normal es que se pidan los nombres y direcciones de quienes la ocuparan y la forma de pago, pero sería muy extraño si, además de esto, se pide información sobre el tipo de sangre de los interesados, sus creencias religiosas y la afinidad que tienen con uno u otro sector de la política. Es allí que la proporcionalidad juega un papel importante, dejando claro que una necesidad de información no puede justificar una entrega total de los datos de la persona, siendo tal acto merecedor de sanción, por destruir el balance que debe existir entre la cantidad de los datos y sus fines.

Así por ejemplo, en el Informe Jurídico 0090-2009 de la Agencia de Protección de Datos se señaló que “la finalidad que ocasiona el tratamiento de datos de localización de un escolta es garantizar la seguridad de la persona escoltada. En este sentido debe recordarse que la prestación del servicio requiere que se mantenga la comunicación entre el empleado y la empresa de seguridad, como resulta de los requisitos exigidos por el Reglamento de

¹⁰⁶ EGUSQUIZA BALMASEDA, Ma. Ángeles, Protección de datos: intimidad y salud, Aranzadi, 2009, p. 126

Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre.... Ahora bien, debe tenerse en cuenta que, el tratamiento de los datos de localización fuera del tiempo de la prestación laboral, resulta excesivo en relación a la finalidad perseguida, por lo que vulneraría el principio de proporcionalidad y resultaría contrario a la LOPD 15/1999”.¹⁰⁷

Para el caso de los temas de salud, estos extremos son un poco más aleatorios, precisamente por la compleja realización de la etapa de “anamnesis”¹⁰⁸ y la “exploración física”, la cual no parece tener parámetros exactos y posiblemente, dependiendo de la patología que sufre el enfermo, sumado al tiempo que asigne el médico a esta etapa, se puede extender o reducir el cuestionario aplicado al paciente, cuya consecuencia se verá reflejada en la cantidad de datos de salud que se lleguen a obtener finalmente. Asimismo, para el caso de enfermedades contagiosas y la generación de sus ficheros, determinar la cantidad de los datos es indispensable, si se quiere lograr el fin propuesto. Por ejemplo, para constituir un fichero sobre enfermos de SIDA, el Tribunal Superior de Justicia de Galicia señaló que no se consideraba excesivo incorporar al registro de este tipo de paciente, los datos sobre “sexo, edad al diagnóstico, fecha de nacimiento, municipio de residencia, fecha del primer resultado positivo confirmado, posibles mecanismos de transmisión y estadio clínico de la infección”, ya que el objetivo propuesto era el control epidemiológico y la recogida de datos para la elaboración de actividades preventivas y profilácticas en esta enfermedad, siendo dichos datos indispensables para cumplir las metas propuestas¹⁰⁹. Dicho sea de paso, se entiende que gracias a los datos del registro se pueden modular los resultados analíticos en función de la probabilidad de que una persona esté afectada o no y no se pretende con ello la discriminación o finalidades distintas de las explicitadas o de que

¹⁰⁷ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0090 – 2009, p.2

¹⁰⁸ Es el documento en el que se refleja la información obtenida de la entrevista inicial realizada al paciente. En la anamnesis se ha de consignar siempre el motivo del ingreso, los antecedentes familiares y los personales que puedan tener relación con la asistencia que se presta, la enfermedad actual y los datos de la exploración física.

¹⁰⁹ STSJ Galicia, 614 – 2008, de 1 octubre, FJ: 4 (RJCA 2009\309)

utilizarlo para servir como sistema de recogida de información generalizada sobre los portadores de VIH/SIDA.

Siguiendo el ejemplo de las enfermedades contagiosas, el principio de proporcionalidad debe evitar la masiva recogida de datos personales que van más allá del puro análisis epidemiológico, evitando el acopio de datos que nada tienen que ver con lo sanitario y que permiten determinar comportamientos de la vida íntima de las personas; así, este principio limita la posibilidad de obtener datos que ayuden a identificar de forma plena a personas concretas (nombre, apellidos, domicilio), cuando los fines y usos previstos pueden lograr perfectamente mediante el acopio de datos disociados o anónimos.

Del mismo modo, teniendo en cuenta el actual grado de avance tecnológico, para evitar excesos en la captación de datos, se pueden establecer códigos anónimos que, salvaguardando la absoluta confidencialidad a que tienen derecho los ciudadanos respecto a datos personales tan sensibles como los recogidos en estos archivos, garanticen a la vez que no se dupliquen los datos epidemiológicos, necesarios para elaborar estadísticas fiables. La gran diferencia con las enfermedades regulares es que el VIH-SIDA aún es causa potencial de discriminación en nuestra sociedad por lo que el acopio injustificado y sin suficiente control de datos especialmente sensibles, supone una fuente de agravios y posible discriminación para los enfermos de SIDA y afectados por esta enfermedad.

Ahora bien, para que exista congruencia entre este tipo de fichero con la garantía constitucional a la intimidad personal “no es suficiente alegar una finalidad de protección de intereses públicos, como antes se ha dicho, pues es preciso cohonestarla con el derecho a la intimidad. De manera que, al adoptar tal medida, es preciso ponderar, adecuadamente y de forma equilibrada, de una parte, la gravedad de la intromisión que comporta en la intimidad

personal y, de otra parte, si la medida es imprescindible para asegurar la defensa del interés público que se pretende proteger”¹¹⁰.

La finalidad en todo caso será la de recuperar su salud y existe la probada necesidad de conocer sus antecedentes de salud, de otro modo, tal como se señala en el Informe Jurídico 0266 – 2006 de la Agencia de Protección de Datos, si dicha finalidad (recuperar la salud), pudiera ser suplida por la realización de una actividad distinta al citado tratamiento (recabar todos los datos del paciente), sin que dicha finalidad sea alterada o perjudicada, debería optarse por esa última actividad¹¹¹. Desafortunadamente, a la fecha es difícil lograr la cura a un enfermo sin conocer previamente antecedentes de su condición física y la de sus familiares, inclusive. Por este motivo, se ha dicho para el caso de los historiales médicos electrónicos, que “la “exhaustividad” de un expediente médico es prácticamente imposible”¹¹², lo cual guarda mucha congruencia con la necesidad de delimitar la cantidad de datos que se incorporan en un fichero de salud.

Sólo como comentario previo al siguiente capítulo sobre la historia clínica, la LOAP 41/2002, en su artículo 15.1, obliga a incorporar en la historia clínica, la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. En ese orden de ideas, señala cuáles son los documentos mínimos que deben incorporarse al expediente, según cada caso, como un esfuerzo para resolver el vacío que existía sobre qué documentos son imprescindibles, pero aún así, no dejan de ser los documentos “básicos” que deben adjuntarse, dejando la opción a que puedan incluirse otros además de los mencionados. Pero, volviendo a la cantidad de los datos, ¿qué es

¹¹⁰ STSJ Asturias, 1333 – 2005, de 12 septiembre, FJ: 8 (RJCA 2007\330)

¹¹¹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0266 – 2006, p. 1

¹¹² Cfr. El Grupo de autoridades de protección de datos, creado por el artículo 29 de la Directiva 95/46/CE, del PE y el CUE, en su Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (documento WP131), adoptado el 15 de febrero de 2007, citado por la Agencia de Protección de Datos en el Informe Jurídico, 0173 -2008, p. 3

“trascendental”?, ¿quién y cómo lo determina? Más allá de los tipos de documentos, aun no queda claro, a mi parecer, cuántos datos debe obtenerse de una persona que sufre una enfermedad, si basta con los datos de salud sobre su estado físico o pueden sumarse otros, como los datos biométricos¹¹³, los perfiles de salud mental, otros, para garantizar una atención adecuada. De allí que el principio de proporción sigue vigente y más para los temas de salud, pues busca mantener ese equilibrio entre protección de los datos, intimidad y derecho a la salud.

La proporción de la entrega y petición de los datos en algunos contratos también definen la validez de estos actos, como es en los contratos de seguros de vida. Aquí, los datos de salud que se obtienen del cliente son determinantes para formalizar dicho contrato, y además de darse alguna omisión a la hora de responder el cuestionario facilitado por la Aseguradora, o no decir la verdad en cuanto el estado de salud, se puede anular la obligación de responder por los daños sufridos por la persona.

5.5.3. Principio de finalidad.

No se puede improvisar con la justificación para recabar los datos, por el contrario debe existir un propósito claramente definido, el cual en ningún momento podrá ser contrarios a derecho y con apego a los permisos que se han otorgado previamente. Es inadecuado el uso de los datos para propósitos no planteados previamente ni para ficheros que no se han aceptado por parte del paciente. Aun así, se mantiene el debate con el concepto “incompatible”, pues podría facilitar el uso de la información de forma inadecuada.

¹¹³ Cfr. El Informe Jurídico 0368 – 2006 de la Agencia de Protección de Datos, destaca que son datos biométricos aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc.

A lo mejor la LOPD 15/1999 pudo decir “diferente”, y así evitar otras interpretaciones que al final desdibujan el interés del legislador por proteger el derecho de la personas. Lo importante en todo caso sería determinar qué se entiende por “incompatible”, para lo cual la lógica nos dice que serían aquellos casos en los que los fines son opuestos entre si, de forma tal que la aplicación de uno impide la existencia del otro. Serían en todo caso excluyentes y no podrían coexistir al mismo momento o para el mismo propósito.

En el Informe Jurídico 0039 – 2010 la Agencia de Protección de Datos analiza si es compatible publicar datos de los trabajadores en la página Web de la empresa, especialmente las evaluaciones hechas por los clientes, con el consentimiento inicial que da el trabajador para iniciar sus labores en la empresa. En este caso la Agencia de Protección de Datos reitera la necesidad de obtener el consentimiento expreso para este propósito, debido a que toda finalidad en el uso de los datos, debe ser previamente explicada y aclarada al interesado, por lo que entiende “que la comunicación de los datos de empleados en Internet, no puede ampararse en el consentimiento del trabajador, en el ámbito de la relación laboral”. Asimismo, este informe jurídico destaca la importancia de la Recomendación (89) 2 del Consejo de Europa, como un documento que ha marcado de forma importante el desarrollo de los temas relacionados con los “fines del empleo”.

5.5.4. Principio de exactitud o veracidad.

No importa lo que somos, sino lo que parecemos ser. En esta máxima radica la importancia de la exactitud de la información: cada dato debe responder a un momento histórico en la vida de su titular, por lo que el principio de veracidad tiene gran relevancia, en cuanto a que los datos se recojan para su tratamiento de acuerdo con una serie de criterios (principio de proporcionalidad) y que los mismos se empleen para finalidades compatibles a las que motivaron la recogida (principio de finalidad), sino que también, los datos han de ser exactos y puestos al día, pues lo contrario supondría de forma implícita el incumplimiento de

los citados principios, con las importantes consecuencias que puede tener para el afectado¹¹⁴. El principio de calidad del dato comienza a infringirse en el momento en que se mantienen datos erróneos¹¹⁵, por eso, existe la obligación del responsable del fichero, en atender el importante aspecto de la actualidad del dato, dar seguimiento y cumplimiento a los objetivos implica revisar periódicamente, el nivel de certeza de la información.

Esta exactitud impide que se proceda con acciones alejadas de derecho, como el caso del usuario que recibe cobros ilegítimos por parte de una empresa, cuyos ficheros no están actualizados. En si la empresa se equivoca y termina cobrando de más al cliente o cobrando a una persona que ni siquiera tiene crédito con ellos. En estos supuestos, “se produce la infracción del mencionado principio de calidad del dato no solo cuando los datos se comunican a los ficheros sobre solvencia patrimonial y crédito (que es el supuesto más frecuente), sino que tal principio de calidad igualmente ha de ser garantizado respecto de los propios ficheros de la entidad acreedora, o de los de otra empresa a la que necesariamente ha de ser comunicada la actualización de los mismos, sin necesidad de ninguna otra comunicación exterior”¹¹⁶. En estos casos el Tribunal ha señalado que la adopción de medidas para la perfecta identificación de los clientes no puede constituir un elemento de atenuación de la responsabilidad, sino que se presenta como el cumplimiento de una obligación ordinaria exigible a las empresas que trabajan con grandes volúmenes de datos personales, sin que pueda considerarse la adopción de estas medidas como base para la apreciar disminución de la culpabilidad ó de la antijuridicidad¹¹⁷.

¹¹⁴ SAN, de 19 noviembre 2008, FJ:4 (JUR 2008\380795)

¹¹⁵ SAN, de 22 julio de 2010, FJ: 2 (JUR 2010\288538)

¹¹⁶ SAN, de 24 junio de 2010, FJ: 5 (RJCA 2010\565).

¹¹⁷ SAN, de 24 junio de 2010, FJ: 7 (RJCA 2010\565). De igual forma, señala que la ejecución del criterio expuesto, aplicado con generalidad, tendría el efecto de beneficiar al infractor reincidente, y el artículo 45.4 de la LOPD 15/1999 ya ha tomado en consideración la reincidencia a los efectos de la fijación del importe indemnizatorio. Por todo ello, y tomando en consideración que la empresa trató los datos del denunciante dándole de alta en un contrato de telefonía, emitiendo determinadas facturas e incluyendo sus datos en un

Esta distancia que existe entre el dato real y el dato incluido en el fichero para los casos de cobros de saldos pendientes es muy común. Pero, además, es contraria a la LOPD 15/1999 ya que el artículo 29.4, “exige que los datos relativos a la deuda sean veraces, esto es, que la deuda exista y en la cuantía fijada y ese principio se infringe en el momento en que se facilitan datos erróneos a un fichero que presta información a terceros sobre el incumplimiento de obligaciones dinerarias”¹¹⁸. De igual forma, aunque existe un plazo de prescripción de la acción del afectado, establecido en dos años por el art. 47 de la LOPD 15/1999, el Tribunal ha sentenciado que “esta infracción participa de la naturaleza propia de las denominadas infracciones continuadas en las que su consumación se proyecta en el tiempo más allá del hecho inicial consistente en el acceso del dato personal erróneo al fichero de solvencia patrimonial, extendiéndose durante todo el período en el que el dato inexacto permanece en el citado fichero, es decir, hasta que deja de producirse dicha lesión a los derechos de afectado, por corregirse la discordancia entre los datos incluidos y la inexactitud del mismo”.¹¹⁹

Las consecuencias de este tipo de error en la calidad del datos son variadas, pero lo más usual es la posibilidad de que se extraiga “una información negativa sobre la solvencia patrimonial y crédito del afectado, pueden por ejemplo, negar, injustificadamente, el acceso a préstamos que le son necesarios para la compra de ciertos bienes, o directamente para su

fichero de morosidad ante el impago de las mismas, a pesar de la voluntad contraria de estas personas al tratamiento de sus datos, resulta que no concurren razones que justifiquen la estimación de los criterios de reducción que resultan del citado artículo 45.5 de la LOPD.

¹¹⁸ SAN, de 16 enero de 2008, FJ: 3 (RJCA 2008\5).

¹¹⁹ SAN, de 23 enero de 2008, FJ: 3 (RJCA 2008\144). Sobre el particular, también dice que esta solución es la única que resulta acorde con la naturaleza del instituto de la prescripción que se encuentra concebida, según reiteradamente ha declarado la jurisprudencia del Tribunal Supremo, como un instituto fundado en razones de seguridad jurídica y no de justicia intrínseca, cuya aplicación se hace depender de la concurrencia del elemento subjetivo de abandono o dejadez en el ejercicio de la propia acción.

adquisición. Además del posible perjuicio patrimonial, existe un daño evidente que afecta al derecho al honor de las personas involucradas cuyos datos de forma ilegítima se incorporan a un registro público que recoge información sobre incumplimiento de obligaciones de pago de dinero”¹²⁰.

Tampoco es ocioso mencionar que, en los casos de créditos o dudas contraídas con empresas, al mantenerse equivocado o desactualizado el dato, mal se puede ceder a terceros esta información con el ánimo de cobro, pues dicha cesión de datos sería considerada “negligente porque previamente no se adoptaron medidas o controles adecuados para verificar la deuda, que hubieran detectado que la misma se había condonado (cancelado) y, por tanto, resultaba (resulta) inexistente en el momento de la cesión de datos personales”¹²¹.

La Agencia de Protección de Datos también emitió reglamentación en esta materia, facultad reglamentaria que se vio reforzada mediante una sentencia del Tribunal Supremo de 16 de febrero de 2007 (RJ 2007\739), en la que señala que la Ley Orgánica 5/1992, otorgó el control de su aplicación a un órgano independiente, al que atribuye el estatuto de Ente público en los términos del art. 6.5 de la Ley General Presupuestaria (la Agencia de Protección de Datos), órgano que, entre otras funciones, tiene la de dictar instrucciones para adecuar los tratamientos a los principios de la ley, función reiterada en el art. 5.c) del Estatuto de la Agencia.

De estos preceptos entiende que se desprende la atribución a la Agencia de Protección de Datos de la facultad de dictar Instrucciones de eficacia "ad extra", en cuanto se dirigen a quienes operan en el tratamiento de datos y resultan de obligada observancia. Instrucciones que son distintas de aquellas a que se refiere el art. 21 de la Ley 30/1992,

¹²⁰ SAN, de 20 septiembre 2002, FJ: 5 (JUR 2003\50000).

¹²¹ SAN, de 30 noviembre 2010, FJ: 4 (JUR 2010\413674)

dirigidas a los órganos jerárquicamente dependientes y destinadas a ordenar las actividades del servicio en virtud de facultades de dirección, que producen efectos "ad intra" y cuya obligatoriedad para los subordinados no derivan de un carácter normativo que no tiene sino de los deberes impuestos en virtud del principio de jerarquía al que responden.

No se trata, por lo tanto, de atribuir a la Agencia de Protección de Datos el desarrollo reglamentario de la ley sino de que la misma, como Ente público al que se encomienda el control de la aplicación de la ley, dirija tal aplicación estableciendo las instrucciones que entienda precisas para conseguir que el tratamiento de datos se ajuste a los principios que la ley dispone, delimitando así el ámbito de la potestad reconocida y con ello de la finalidad y objeto de tales instrucciones, que se proyectan sobre la aplicación de la ley, al margen, por tanto, de su desarrollo reglamentario mediante las correspondientes disposiciones generales, en el que la intervención de la Agencia se limita a la emisión de los correspondientes informes. En definitiva la Instrucción 1/1995 tiene la consideración de norma reglamentaria a los efectos de integración del tipo infractor previsto en el art. 44.3.d) de la LOPD.

De esta manera, mediante Informe Jurídico 1/1995¹²² de la Agencia de Protección de Datos, norma primera, se establecen las siguientes condiciones previas a la inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

1. Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada.

2. Requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación. No podrán incluirse en los ficheros de esta naturaleza datos

¹²² AGENCIA DE PROTECCIÓN DE DATOS, Instrucción 1/1995, de 1 de marzo, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.

personales sobre los que exista un principio de prueba documental que aparentemente contradiga alguno de los requisitos anteriores. Tal circunstancia determinará igualmente la desaparición cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.

3. El acreedor o quien actúe por su cuenta e interés deberá asegurarse que concurren todos los requisitos exigidos en el número 1 de esta Norma en el momento de notificar los datos adversos al responsable del fichero común.

4. La comunicación del dato inexistente o inexacto, con el fin de obtener su cancelación o modificación, deberá efectuarse por el acreedor o quien actúe por su cuenta al responsable del fichero común en el mínimo tiempo posible, y en todo caso en una semana. Dicho plazo es independiente del establecido en el artículo 15.2 del Real Decreto 1332/1994, de 20 de junio, y que se aplica al fichero del acreedor.

Por otro lado, la LOPD 15/1999, establece sanciones por la inexactitud del dato, como bien expone la Audiencia Nacional¹²³. Lo que sanciona el artículo 44.3.d) es el tratamiento de los datos de carácter personal o su uso posterior con conculcación de los principios y garantías establecidos en la LOPD 15/1999 o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, por lo que debe relacionarse dicho tratamiento con el resto de garantías previstas en la ley y que se relacionan con las previstas en los artículos 4.3 y 29.4.

En relación con lo anterior, la misma sentencia la Audiencia Nacional señala que, aquel que utiliza un medio extraordinario de cobro como es el de la anotación de la deuda en un registro de morosos, debe garantizar el cumplimiento de todos los requisitos materiales (exactitud del dato) y formales (requerimiento previo) que permitan el empleo de este modo

¹²³ SAN, de 24 octubre 2007, FJ: 3 (RJCA 2008\122)

accesorio para conseguir el cobro de la deuda. No aplicar esta exigencia supondría, por el contrario, utilizar este medio de presión al recurrente sin el suficiente aseguramiento de las mínimas garantías para los titulares de los datos que son anotados en los registros de morosos.

En si, la inexactitud en los datos también pondría en evidencia la falta de diligencia demostrada por el Responsable del Fichero, por no asegurarse antes de incorporar o ceder los datos, que la calidad del dato de la persona sea congruente con la situación real que refleja. Por tanto, tal omisión en la conducta es susceptible de sanción, pues se configura el elemento culpabilístico de la infracción administrativa y resulta imputable cuando se reclame. Además, la LOPD 15/1999 ha sido clara en cuanto a la comprobación de la exactitud del dato, es decir, que tal previsión debe realizarse previamente y de modo riguroso, para evitar causar cualquier tipo de daño al titular de los datos.

En estos casos, dentro la conducta adecuada que se espera del responsable del fichero está que mantenga actualizados sus datos y cumpla con el deber legal de cuidado sobre la información que posee. Es decir que contrario a lo normal, permitir la incorporación y vigencia en sus ficheros de un dato inexacto, no corresponde con la diligencia que se espera por su parte. Asimismo, dado que a éste se le exige el control principal de los datos, debe tener un dominio total de la información que acumula, y es lógico que se insista en el exquisito cuidado de sus labores, para poder ajustarse a las prevenciones legales al respecto.

El Tribunal Supremo también ha reiterado que, en estos casos, “se deben extremar las cautelas a la hora de tratar dichos datos, especialmente cuando los datos objeto de tratamiento son datos de salud...”¹²⁴. Aquí el Tribunal hace alusión al cuidado que debe tener una empresa asegurada al momento de remitir, por correspondencia, alguna información de salud de sus clientes, de lo cual exige especial atención con los datos de

¹²⁴ STS, de 10 junio 2011, FJ: 1 (RJ 2011\5195)

domicilio para no equivocarse con el envío de información tan sensible y evitar la pérdida o la cesión involuntaria de datos a personas distintas al titular.

Por estos motivos, también se espera que el Responsable del Fichero conozca adecuadamente las normas que reglamentan la actividad que desarrolla diariamente y en ningún caso puede invocarse su desconocimiento para justificar o atenuar sus obligaciones. Ya se ha reiterado que las consecuencias negativas las asume en su mayoría la persona dueña de los datos, lo que estaría totalmente en contra de las garantías que el propio derecho ha desarrollado en esta materia.

5.5.5. Principio de conservación.

Los datos de salud deben ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos. En definitiva, todo dato tiene un periodo de vigencia o por lo menos de uso útil, lo que, una vez cumplidos los objetivos, debe procederse al descarte de la información.

Para lograr esto, primero debe tenerse un control exacto de los datos y a quién pertenecen, posteriormente, identificar si se han cumplido los objetivos y, de ser así, proceder con su cancelación, salvo los fines estadísticos o históricos, de los cuales se pretende utilizar para objetivos variados, desde inversión de gastos, generación de estudios, o simplemente control de los recursos asignados en la protección de la salud.

6. Regulación autonómica de la protección de los datos personales.

La Comunidad Autónoma de Madrid, Cataluña y País Vasco, siguiendo la autorización brindada por la LOPD 15/1999, aprobaron de forma separada, la creación de agencias autonómicas en sus respectivas comunidades, responsables de velar por la protección de los datos de sus habitantes.

6.1. La Comunidad Autónoma de Madrid.

La Comunidad Autónoma de Madrid, mediante la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, optó por desarrollar de manera particular todas aquellas materias para las cuales encontró una habilitación concreta en la propia LOPD 15/1999.

La regulación del procedimiento de elaboración de las disposiciones que creen, modifiquen o supriman ficheros de titularidad de la Comunidad de Madrid; la delimitación de las funciones, organización y régimen jurídico básico de la Agencia de Protección de Datos de la Comunidad de Madrid; cooperación interadministrativa y otros aspectos relacionados con la seguridad. Por tal motivo, advierte la Exposición de Motivos, se suprimió todas las referencias contenidas en la Ley 13/1995, de 21 de abril, en relación a cuestiones como recogida de datos de carácter personal, derechos de los ciudadanos y principio del consentimiento, ejercicio de los derechos de acceso, cancelación y rectificación, cesión de datos, etcétera, que ya están reguladas en la LOPD 15/1999, pues son aspectos esenciales que delimitan el sistema de protección de las libertades públicas y los derechos fundamentales de las personas físicas, especialmente el derecho al honor y a la intimidad personal y familiar, en el tratamiento de los datos personales.

La Agencia de Protección de Datos de la Comunidad de Madrid ejerce sus funciones de control sobre los ficheros de datos de carácter personal creados o gestionados por las Instituciones de la Comunidad de Madrid y por los Órganos, Organismos, Entidades de Derecho público y demás entes públicos integrantes de su Administración Pública, exceptuándose las sociedades mercantiles a que se refiere el artículo 2.2.c).1 de la Ley 1/1984, de 19 de enero, reguladora de la Administración Institucional de la Comunidad de Madrid.

Asimismo, dichas funciones se ejercerán sobre los ficheros de datos de carácter personal creados o gestionados por los entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, de conformidad con lo previsto en el artículo 41 de la LOPD 15/1999 así como sobre los ficheros creados o gestionados por las Universidades públicas y por las corporaciones de derecho público representativas de intereses económico y profesionales de la Comunidad de Madrid, en este último caso siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público

Los ficheros regulados por la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, creados o gestionados por las entidades y empresas de la Comunidad de Madrid y Entidades Locales referidos en el apartado anterior, para fines no estatales, se regirán por dicha disposición en defecto de la legislación estadística de que pueda dotarse la Comunidad de Madrid, pero estarán sometidos al control de la Agencia de Protección de Datos de la Comunidad de Madrid.

6.2. La Comunidad Autónoma de Cataluña.

La Comunidad Autónoma de Cataluña, mediante Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de la Protección de Datos, también desarrolló de manera particular la protección de los datos en los temas que le corresponde. Tal como se menciona en el

preámbulo de esta ley, la Agencia Catalana de Protección de Datos, es una autoridad independiente creada por la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, y desde su creación veló por la garantía del derecho a la protección de datos en el ámbito de las administraciones públicas de Cataluña mediante el asesoramiento, la difusión del derecho y el cumplimiento de las funciones de control establecidas por el ordenamiento jurídico.

Esta Agencia posee competencias de registro, control, inspección, sanción y resolución, así como la aprobación de propuestas, recomendaciones e instrucciones, en especial para los siguientes tipos de ficheros:

a) Las instituciones públicas.

b) La Administración de la Generalidad.

c) Los entes locales.

d) Las entidades autónomas, los consorcios y las demás entidades de derecho público vinculadas a la Administración de la Generalidad o a los entes locales, o que dependen de ellos.

e) Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalidad, a los entes locales o a los entes que dependen de ellos:

Primero. Que su capital pertenezca mayoritariamente a dichos entes públicos.

Segundo. Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos.

Tercero. Que en sus órganos directivos los miembros designados por dichos entes públicos sean mayoría.

f) Las demás entidades de derecho privado que prestan servicios públicos mediante cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de dichos servicios.

g) Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que de ellas dependen.

h) Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalidad o de los entes locales, si se trata de ficheros o tratamientos destinados al ejercicio de dichas funciones y el tratamiento se lleva a cabo en Cataluña.

i) Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña a los efectos de lo establecido por la presente ley.

En ese mismo orden de ideas, esta Agencia de Protección de Datos Catalana encuentra fundamento jurídico en la aprobación del Estatuto de autonomía de 2006, lo cual supuso el reconocimiento expreso, por vez primera en el ámbito estatutario, del derecho a la protección de datos y reforzó el papel de la autoridad de control en materia de protección de datos, ya que, por una parte, clarificó y amplió su ámbito de actuación y, por otra, reforzó su independencia al establecer su designación parlamentaria.

6.3. La Comunidad Autónoma del País Vasco.

El País Vasco por su parte, mediante Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, desarrollada mediante Decreto 308/2005, de 18 de octubre, reglamentó esta materia en su respectiva área de competencia.

Sobre el particular, la ley Vasca es aplicable a los ficheros de datos de carácter personal creados o gestionados, para el ejercicio de potestades de derecho público, así:

a. La Administración General de la comunidad autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad

Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público.

b. El Parlamento Vasco.

c. El Tribunal Vasco de Cuentas Públicas.

d. El Ararteko.

e. El Consejo de Relaciones Laborales.

f. El Consejo Económico y Social.

g. El Consejo Superior de Cooperativas.

h. La Agencia Vasca de Protección de Datos.

i. La Comisión Arbitral.

j. Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco.

k. Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario.

2.- No obstante lo dispuesto en el número anterior, esta ley no será de aplicación a los ficheros:

a. Sometidos a la normativa sobre protección de materias clasificadas.

b. Establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

c. Regulados por la legislación de régimen electoral.

d. Procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por los cuerpos de Policía del País Vasco, de conformidad con la legislación sobre la materia.

El amplio desarrollo normativo que han tenido estas agencias autonómicas exceden los límites que se han planteado en la presente investigación, pero es importante señalar que todas han tenido un papel relevante en la protección de los datos de las personas y han emitido múltiples resoluciones, informes, y documentación variada, cuyo fin ha sido ampliar y responder ante el ciudadano por la protección de sus derechos.

7. Resumen de ideas.

Dentro de este primer capítulo se ha presentado la importancia que tienen los datos para las personas. El impacto que ha tenido la tecnología en el manejo de la información, que trajo como consecuencia que el derecho ampliara su haz de protección hacia un nuevo sector como son los datos personales.

Aunque existen muchos escenarios en los que los datos cobran extremado valor, en esta investigación avanzará hacia un sector en especial, nos referimos a los datos personales del paciente, o los llamados datos de salud.

Esta elección no es a la ligera, y se corresponde con la distinción que la propia LOPD 15/1999, hace a este tipo de datos, en cuanto a su importancia y la obligación de mantenerlos con altos niveles de seguridad para su conservación.

Pero, ¿por qué este sector es importante para la protección de los datos? A esto hay que decir que el ámbito de la salud se consolida como uno de los mayores sectores de la

economía mundial. Según la Organización Mundial de la Salud, el sector alcanzó US\$5,5 trillones en 2009, absorbiendo el equivalente al 8% del PIB mundial. Por esto, no es de extrañar que la información concerniente a la condición de salud de una persona, resulte de gran importancia para planificación y desarrollo de políticas públicas, aunado al peso que representa para la economía de las empresas y los particulares.

Y es que en todo caso, la cobertura mundial de la salud se está incrementando, ahora existen más áreas de atención para el paciente y hasta se realizan de manera compartida entre los países de la unión, mediante el sistema de historia clínica electrónica. Este supuesto implica inmediatamente todo un reto para los países, lograr encontrar un balance entre sus obligaciones como país, participante en el conjunto como comunitario y las obligaciones que asume con particular.

Aunado a lo anterior, existe la necesidad de control del ciudadano sobre sus propios datos como un derecho fundamental poco atendido por los responsables, pero de una gran importancia en el momento en el que vivimos. A diario, cualquier decisión que tomemos que implique una cierta trascendencia jurídica, conlleva el acceso a nuestros datos personales: si solicitamos atención médica, tenemos que facilitar como mínimo, nuestro nombre y apellidos y así sucesivamente para cada servicio se archivará nuestra información en un compendio que será accesible a muchas personas.

En el próximo capítulo se analizará la normativa vigente en esta materia, los datos de salud en sí, y algunos ejemplos de ellos, los cuales han cobrado mayor vigencia, con la incorporación de esas nuevas tecnologías ya mencionadas.

De igual forma, veremos la importancia de la voluntad del paciente y su capacidad de decidir sobre la utilización de su información, y se tomará como ejemplo aquellos casos en los que el trabajador debe decir sobre su información de salud.

CAPITULO 2

LOS DATOS DE SALUD

Sumario: 1. Aproximación al tema. 2. Marco normativo aplicable a los datos de salud. 2.1. Normativa comunitaria. 2.2. Legislación estatal en materia de salud. 2.3. Otras normas protectoras de los datos de salud. 3. La protección de los datos de salud. 3.1. Definición del dato de salud. 3.2. Datos especialmente protegidos. 3.3. Datos de salud del menor de edad. 3.4. El dato de salud y las nuevas tecnologías. 3.5. Los datos de salud – genéticos. 4. Obligación de disociar el dato salud. 4.1. El esfuerzo desproporcionado. 4.2. La opinión del paciente para disociar el dato de salud. 4.3. Obligación de disociar para investigación. 4.4. Obligación de disociar para casos judiciales. 4.5. Obligación de disociar para docencia. 5. El consentimiento para el uso de los datos de salud. 5.1. Revocación del consentimiento: un derecho del paciente a decir no. 5.2. Excepciones al consentimiento en el uso del dato de salud. 5.2.1. Excepciones al consentimiento y uso de datos de salud del trabajador. 5.2.1.1. El reconocimiento para evaluar los efectos de las condiciones de trabajo sobre la salud. 5.2.1.2. Reconocimiento para comprobar si el estado de salud del trabajador constituye un peligro para su integridad, la de sus compañeros o terceros. 5.2.1.3. Reconocimientos obligatorios por disposición legal. 6. Índice de cumplimiento de la protección de datos de salud. 7. Resumen de ideas.

1. Aproximación al tema.

En el primer capítulo se analizó la importancia de los datos personales, se hizo hincapié en el reconocimiento internacional a este nuevo derecho fundamental y también se abordó el amplio debate surgido con el reconocimiento de este derecho en la Legislación española.

Existen muchas clases de datos y su clasificación podría determinarse por el contenido de la información que encierran. Sin embargo, es importante señalar que los datos individuales son generalmente inofensivos, sobre todo si su significado no es claro y requiere de otros datos para cobrar valor. Es la suma de ellos lo que complica la situación, dado que al unirse pueden generar un perfil que exponga, sin consentimiento, a su titular.

Dentro de los tantos datos que existen están los datos de salud que por sus características propias, pueden estar organizados en diversos ficheros, de hospitales, compañías de seguro y el propio Estado. Ahora bien, mediante este tipo de dato “otros” pueden conocer la condición de una persona en particular, su enfermedad y la forma cómo asume el reto de su tratamiento y su recuperación. A lo mejor, el dato de salud no es el más complicado, si se coloca en la balanza frente a otros como son: la elección religiosa, la tendencia política y demás; pero, al igual que un dato económico, su impacto en la persona y en la sociedad puede llegar a tener efectos devastadores.

En ese sentido, la investigación también justifica su elección, ya que el manejo inadecuado de este tipo de dato puede inclusive cambiar la autoestima del paciente, haciéndolo ver las cosas positiva o negativamente, puede afectar las perspectivas que tiene de si mismo y como consecuencia, cambiar su comportamiento. Además, el pobre control de los datos conlleva injerencias arbitrarias o ilegales en la vida privada, así como la utilización de los datos personales para fines distintos por los que fueron recabados en primera instancia. Entre estos datos de salud, habrá algunos insignificantes y otros no, pero en su gran mayoría, todos cobran significado ante la manipulación de la información que se promueve en algunos sectores.

Por otro lado, por ejemplo, si un médico va a realizar una cirugía, y para esto cuenta con información errónea, incompleta, fragmentada, inaccesible o en definitiva no compatible con el paciente, es casi probable que el médico cometa errores, cuya

consecuencia asumirá el enfermo. Por esto, es imprescindible resaltar la necesidad de que, tanto en los hospitales públicos como privados se cumpla con los principios de protección de datos de salud, ajustando todos los criterios de seguridad y calidad de la información

En definitiva, hoy la información es un recurso básico en las instituciones sanitarias, tan o más importante como el presupuesto económico del propio hospital. Y, al igual que cualquier otro recurso, es importante mantener su custodia en forma adecuada, para garantizar que el derecho a mantener los datos en custodia, se cumplirá durante todo el tiempo que sea necesario.

Ahora más que nunca es necesario proteger la información y la intimidad de los pacientes, sobre todo cuando se tiene al alcance las tecnologías de la información. En ese estudio, se abordarán: el concepto de dato de salud, algunos ejemplos de ellos, su regulación, los datos genéticos y la necesidad de contar con una protección adecuada para estos ficheros.

2. Marco normativo aplicable a los datos de salud.

2.1. Normativa comunitaria.

Iniciamos este punto refiriéndonos a las normas que propulsaron la protección de los datos de salud. El Convenio sobre los derechos humanos y la biomedicina - convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la biología y la medicina, suscrito en Oviedo el 4 de abril de 1997, fue determinante en este aspecto, pues aporta bases para la protección de los datos del paciente. En su artículo 5 establece como regla general, que la intervención en el ámbito de la sanidad sólo podrá efectuarse después de que la persona afectada haya dado su libre e informado consentimiento. Dicha persona deberá recibir previamente una información

adecuada acerca de la finalidad y la naturaleza de la intervención, así como sobre sus riesgos y consecuencias. En cualquier momento la persona afectada podrá retirar libremente su consentimiento.

Sobre nuestro tema en concreto, en el capítulo III de este Convenio, sobre vida privada y derecho a la información, el artículo 10 señala que “Toda persona tendrá derecho a que se respete su vida privada cuando se trate de informaciones relativas a su salud y tendrá derecho a conocer toda la información obtenida respecto a su salud. No obstante, aclara este artículo, se deberá respetar la voluntad de una persona de no ser informada. Asimismo, de modo excepcional, la ley podrá establecer restricciones, en interés del paciente, con respecto al ejercicio de los derechos mencionados en el apartado 2 del Convenio.

La Directiva 95/46/CE, del PE y el CUE aprobó, en su sección tercera, sobre las “Categorías Especiales de Tratamiento”. El artículo 8.1 que dice: “los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.” Sin embargo, aunque esta información es privilegiada, esta misma directiva matiza su contenido y establece varias excepciones a lo señalado en el artículo 8.1, pues el siguiente párrafo dice, 8.2. a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado; o b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas; o c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías

por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados; o e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

El artículo 8.3 de esta Directiva 95/46/CE, del PE y el CUE, señala la excepción al cumplimiento, específicamente cuando el tratamiento de datos 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 sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto. Posteriormente, la Directiva 95/46/CE, del PE y el CUE, en su artículo 8, sólo se refiere a los datos de salud, al incluirlos entre los datos que conforman la categoría de “especial tratamiento” y tampoco entra a definir el concepto.

Es correcto pensar que ante el derecho individual existe el derecho colectivo y, aunque una persona vea afectado su derecho a la privacidad de sus datos, si de éste depende la convivencia saludable con el resto de las personas, la ley tendrá que ponderar los intereses en juego, probablemente pronunciándose en favor al derecho común que en relación con el individual. En si, es muy importante que la ley haga las diferencias a fin de que el individuo no imponga su derecho por encima de la afectación del resto de ciudadanos.

Asimismo, la propia gestión de los servicios de salud, estará condicionada al tipo de información, por lo cual, manteniendo controles, como el caso del secreto médico, se

puede hacer uso de éstas afectando lo menos posible. La apuesta del Estado está dirigida a garantizar la sanidad completa y responsable de la población y que ésta reciba formación y protección continuada y permanentemente, revisando constantemente los resultados que se esperan en cada caso. La excepción que hace la norma, en dar valor a la salud en general, debe entenderse en el sentido más amplio, pero menos perverso, pues no se trata de una simple intromisión en los datos sanitarios de un ciudadano, sino más bien, de los controles básicos para asegurar la correcta gestión de la sanidad, y que estos objetivos están alineados con los que tiene la propia sociedad.

Para adaptarse a esta excepción es necesario determinar, cuándo es permisible hacer estas diferencias y cuándo estamos ante una intromisión ilegal. Esto podría redibujar la función y el modelo que propone la propia Directiva 95/46/CE, del PE y el CUE y, en general, el derecho aplicable al ciudadano, imponiendo a la vez nuevos niveles de afectación hacia sus derechos.

Por otro lado, el Convenio 108, del Consejo de Europa, no hizo referencia a la definición de datos de salud, y aunque el artículo 2 se refiere a las definiciones, sólo se refiere a nuestro tema, en cuanto a que no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. A esto hay que mencionar que para aclarar el alcance de este concepto debía acudir al apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa en la que se considera que el concepto de datos de carácter personal relativos a la salud abarca las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo, pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido; añadiendo que debe entenderse que estos datos comprenden, igualmente, las informaciones relativa al abuso del alcohol o al consumo de drogas.

Debido a estos vacíos jurídicos anteriores, la LOPD 15/1999, principal norma que podría definir el concepto de dato de salud, tampoco lo hizo, pues aunque en el artículo 7.3, refiere a los datos de salud, como información sensible, sujeta a mayor cuidado, no entra a definir dicho concepto. Esta ausencia dejaba cierta ambigüedad en torno al concepto y sobre todo a su real alcance, si se refiere al estado actual, pasado o futuro de la persona.

2.2. Legislación estatal en materia de Salud.

Entrando ya en el derecho positivo Español, es importante reconocer el alto valor que tiene la LGS 14/1986 debido a que destacó el derecho a la salud que tienen todos los pacientes, tanto así que en su exposición de motivos señalaba que “la ley daba respuesta al primer requerimiento constitucional aludido, reconociendo el derecho a obtener las prestaciones del sistema sanitario a todos los ciudadanos y a los extranjeros residentes en España...”

En relación con el tema de esta investigación, en su artículo 10. 3 ya reconocía el derecho que tiene el paciente a la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público. Asimismo, en el apartado 11, estableció la obligación de dejar constancia por escrito de todo su proceso y al finalizar la estancia del usuario en una institución hospitalaria, el paciente, familiar o persona a él allegada recibiría su informe de alta. Posteriormente, se aprobó la LOAP 41/2002, como una norma innovadora, que “asume plenamente el cambio sociocultural en la manera de entender la relación clínica que se ha consolidado paulatinamente en los últimos años, con el tránsito desde el tradicional paternalismo médico hacia un planteamiento centrado en la autonomía del paciente, y viene a clarificar un escenario sin duda complejo que resulta poco matizado legalmente con

anterioridad, aportando en consecuencia importantes dosis de seguridad jurídica sobre la materia”¹²⁵.

Sobre los datos de la salud, la LOPD 15/1999, en su artículo 7.3 señala que “los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente”. En ese sentido, el artículo 8 de la LOPD 15/1999 también dice 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”.

Del mismo modo, la LOPD 15/1999, también reconoció en su artículo 10, la obligación para “el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo”. Este tema lo abordaremos con más detalle posteriormente.

De igual forma, no se requerirá el consentimiento de la persona, tal como lo señala el artículo 11.2.f, “cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica”.

¹²⁵ PEMAN GAVÍN, Juan María, Asistencia sanitaria y sistema nacional de salud, Edit. Comares, Granada, 2005, p.309.

La Comunidad de Madrid ha aprobado una regulación general propia sobre la protección de los datos, mediante Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. Sin embargo, esta ley no hace alusión a la definición de dato de salud, siendo un elemento que se echa en falta en la redacción de una norma tan importante. Además, de la Comunidad Autónoma de Madrid, Cataluña y País Vasco han desarrollado también sus propias normativas en el ámbito de la protección de datos, mediante Ley 5/2002 de 19 de abril, de la Agencia Catalana de Protección de Datos y la Ley 2/2004 de 25 febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, respectivamente. Hay que señalar que sólo la Ley 2/2004 del País Vasco hace alusión a la gravedad de utilizar sin consentimiento los datos de salud; en su artículo 22.4. d) dice que se considera una falta grave “recabar y tratar datos referidos al origen racial, a la salud o a la vida sexual, cuando no lo disponga una ley o el afectado no haya consentido expresamente”. Esto lo desarrollaremos con más detalle en un próximo apartado.

También, con el avance de los años, se puede notar cómo en las normativas más recientes sí se incluyen referencias directas a los datos de salud. Tal es el caso del Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica de la Comunidad Autónoma de Galicia, que en su artículo 5, apartados uno y dos señala que “Los datos de salud, en cuanto datos especialmente protegidos, podrán tratarse y cederse en los términos previstos en los artículos 7, 8 y 11 de la LOPD 15/1999, y su reglamento aprobado por el Real Decreto 1720/2007”. Y añade que, “en particular, no será necesario el consentimiento de la persona interesada para la comunicación de datos personales sobre la salud a través de medios electrónicos, entre organismos, centros, servicios y establecimientos de la Consellería de Sanidad, el Servicio Gallego de Salud y el sistema nacional de salud, cuando se realice para llevar a cabo la atención sanitaria de las personas, tanto se realice con medios propios o concertados”.

Por último, este vacío jurídico en el concepto de dato de salud fue solucionado afortunadamente, mediante la aprobación del Real Decreto 1720/2007, el cual en su artículo 5, apartado g), define “datos de carácter personal relacionados con la salud a las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética”. Debo decir que considero afortunado incluir esta definición, pues trae consigo una gran solución a las múltiples interpretaciones que se daban anteriormente al concepto, algunas más extensas que otras y que en ocasiones traían como consecuencia una mayor o menor protección al derecho del paciente. Siendo así, creo que es importante que se incluyan este tipo de definiciones en la normativa, pues ayudan a guiar al lector para comprender el alcance que tiene la norma y la intención que buscaba el parlamento con su aprobación. Ahora bien, entiendo que con este criterio no coincide DAVARA RODRIGUEZ, quien ha dejado clara su oposición a este tipo de redacción de definiciones, por considerarlas que “ponen límites de alguna forma a la más amplia interpretación y, por tanto, recorta la extensión del espíritu de la ley en su aplicación práctica”¹²⁶, aunque matiza que en algunos casos son necesarias, por ser materias novedosas.

Teniendo claro el concepto, podemos inferir que la información contenida en los historiales clínicos, de manera general, puede ser considerada como datos relativos a la salud, pero este mismo concepto todavía está sujeto a múltiples interpretaciones. Por ejemplo, en ocasiones, a esta información contenida en los historiales clínicos se les llaman: datos de salud, datos sanitarios, inclusive datos médicos, lo cual implica ciertas diferencias, entre si, si analizamos con detalles la materia que abarcan tales denominaciones.

¹²⁶ Cfr., DAVARA RODRÍGUEZ, Miguel A., La protección de datos personales en el sector de las telecomunicaciones, Universidad Pontificia de Comillas, 2000, pp. 13 y 14.

En sí, todos los términos parecen aludir a un mismo punto central, “la salud”. Haciendo un análisis más detallado, podríamos encontrar algunos elementos particulares. Así, el dato de salud está directamente referido o vinculado con la información del enfermo/paciente. Sin embargo, cuando se habla de dato sanitario, pareciera que se hace mayor referencia al dato obtenido mediante el trámite de la sanidad, o sea, la atención que brinda el Estado a sus ciudadanos, mediante las instancias sanitarias. Por otro lado, el dato médico está directamente asociado a la participación de un profesional de la medicina, el cual en uso de su arte o mediante la investigación, logra identificar las características que presenta en enfermo, en un momento determinado.

No obstante, aunque hemos reconocido que los diferentes adjetivos que se le han acuñado al concepto de dato de salud, como el “sanitario” y el “médico”, pueden tener elementos en común, hay que reconocer que no todo dato de salud, es siempre sanitario o médico. Un claro ejemplo de esto son los datos de salud que pudiese manejar un profesional de la acupuntura o un curandero sobre sus pacientes, pues por ejercer de manera privada fuera del organigrama estatal no se constituye en dato sanitario y dado que no son profesionales de la medicina, tampoco podría considerarse como datos médicos.

Más allá de los diversos adjetivos, no debemos alejarnos de lo que más interesa al ciudadano, que es preservar su información de salud como paciente, poniendo a su disposición todas las alternativas para su efectiva protección, frente al ataque a la privacidad o los intereses particulares de terceros, quienes trataran de lograr algún tipo de beneficio, directo o indirecto.

2.3. Otras normas protectoras del los datos de salud.

Además de estas normas estatales y autonómicas, existen otras vinculadas a la materia sanitaria, que igualmente prevén el derecho a la intimidad y el resguardo de los datos de salud del paciente, entre ellas enunciamos muy brevemente las siguientes:

1. La Ley 16/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida y la Ley orgánica 2/2010, de 3 de marzo, sobre salud sexual y reproductiva y de la interrupción voluntaria del embarazo (art. 20 – 23).
2. Real Decreto 411/1996, de 1 de marzo, por el cual se regulan las actividades relativas a la utilización clínica de tejidos humanos (art. 3.1, 3.2. 3.3).
3. El Real Decreto 2070/1999, de 30 de diciembre, por el que se regulan las actividades de obtención y utilización clínica de órganos humanos y la coordinación territorial en materia de donación y trasplante de órganos y tejidos (5.1. 5.2, 5.3).
4. El Real Decreto 1088/2005, de 16 de septiembre, por el cual se establecen los requisitos técnicos y condiciones mínimas de la hemodonación y de los centros y servicios de transfusión (art.5.1).
5. El Real Decreto 1301/2006, de 10 de noviembre, 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 (6.1, 6.2, 6.3, 6.4 y 6.5).

6. El Real decreto 223/2004, de 6 de febrero, por el que se regula los ensayos clínicos con medicamentos (art. 3.6, 18.3 y 21).

3. La protección de los datos de salud.

La protección de los datos, y en especial los datos de salud, son temas que cada vez toman más valor en la palestra pública. El ciudadano en particular y la propia organización estatal buscan resguardar estos nuevos derechos, aunque el camino para su defensa total parece complejo y sujeto a constantes ajustes, debido en parte al “gran conflicto entre la libertad de información y de tratamiento de datos, junto a la libertad de expresión y la intimidad, que genera a su vez grandes y graves discrepancias doctrinales¹²⁷”. Esta confrontación de derechos fundamentales ha sido analizada ampliamente por el derecho y sólo encuentra salida en el análisis individual de cada caso, sin desconocer que conforme a la demanda social se podría llegar a la ponderación de derechos, para facilitar el acceso a una respuesta justa y la protección de todos los intereses en conflicto.

Aunque existe una ley especial para proteger los datos personales de forma general, que en uno u otro artículo se refiere a los datos de salud y una ley especial para proteger los derechos de los pacientes, no existe una ley que resuma de manera completa ambos intereses en un solo texto, no existe a la fecha una ley especial de protección del dato de salud. A lo mejor el propio sistema anima a que esta condición jurídica sea la más adecuada, pero estamos convencidos que con el movimiento globalizante que existe actualmente, los grupos parlamentarios y el propio estamento judicial tendrá que ir afinando el lápiz en este sentido. Sobre lo anterior, entendemos que lo más importante a rescatar de ambas legislaciones no será solamente cómo se obtiene y protege una información de salud, eso ya lo iremos viendo durante la investigación para mí, lo más importante es “el

¹²⁷ DAVARA RODRÍGUEZ, Miguel A., La protección de datos personales en el sector de las telecomunicaciones, Universidad Pontificia de Comillas, Op. Cit., p.9

conocimiento *per se*”, aquello que no reposa o está encadenado únicamente en un documento, físico o digital, o guardado en un fichero. Lo más importante, a mi criterio, es destacar la importancia de proteger al enfermo del conocimiento y la opinión de terceros. Lo peligroso que es que dicho conocimiento se pueda desplazar libremente, independientemente del medio que se utilice y si se posee o no una historia clínica, parcial o completa, por ejemplo. El peligro nace cuando alguien sabe ilegalmente lo qué padece el paciente, cómo lo padece, desde cuándo lo padece y cuál es el sufrimiento que le causa. Allí está, a mi parecer, el *sustratum* de la protección del dato de salud, en el sufrimiento que vive el paciente y que “quizás” no quiere compartir, por lo que se niega a que otros puedan usar tal información en su contra o para otros provechos.

Ante esta situación, también es importante hacer una evaluación de los principales componentes de ambas leyes y desarrollar a partir de ellos una idea de texto único, para construir lo que sería el derecho especial a la protección del dato de salud y su tratamiento adecuado en los ficheros públicos y privados. Asimismo, esta compilación debe hacerse desde la importancia que tienen los derechos de los pacientes como eje básico de las relaciones clínico-asistenciales, entre los cuales resaltan el derecho a la información, el consentimiento informado y la intimidad relativa a la salud de las personas. De este modo, la organización jurídico sanitaria debe “garantizar la salud como derecho inalienable de la población mediante la estructura del Sistema Nacional de Salud, que debe asegurarse en condiciones de escrupuloso respeto a la intimidad personal y a la libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan y sin ningún tipo de discriminación¹²⁸”.

En si, esta temática surge porque todos sufrimos enfermedades y en consecuencia, tenemos la necesidad de aportar información personal, con el propósito de recuperar el estado óptimo de bienestar físico y mental. Esta información estará contenida

¹²⁸ STSJ Asturias, 1165 – 2008, de 30 septiembre, FJ: 4 (RJCA 2009\308)

regularmente en el historial clínico, del cual hemos hablado en capítulos anteriores, mismo que puede incorporar múltiples elementos, tanto documentales como de otro tipo¹²⁹. Y es que, en todo caso, nuestra salud en todas sus modalidades, siempre será una de las variables que determinará si logramos o no las metas propuestas, por lo que su importancia no tiene discusión frente a otros temas de parecido interés.

Si bien ahora hablamos de la protección de los datos de salud como un derecho fundamental, que es diferente, autónomo y más complejo¹³⁰ que el derecho fundamental a la intimidad, hay que reconocer que otorgar esta categoría no ha sido fácil, sobre todo por la relevancia que tienen los “derechos fundamentales”, en la Constitución Española, ya que aquellos son de gran importancia, a su vez dan cuerpo y orientación al resto de derechos consagrados en la Carta Magna. En definitiva, el derecho fundamental a la protección de los datos de salud, ahora reconocido en propiedad, nace del derecho fundamental a la protección de los datos, tema que ya hemos analizado, sobre todo por el amplio debate surgido a partir de la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

¹²⁹ SAN, de 3 febrero 2011, FJ:2, (JUR 2011\58366), llama la atención que en esta sentencia se reconoce que, en materia de documentación clínica, unos botes con muestras orgánicas relativas a pacientes, claramente se equiparan a documentación clínica, por lo que resulta de aplicación lo que establece en la LOPD 15/1999 y su normativa de desarrollo.

¹³⁰ GARRIGA DOMIGUEZ, Ana, “La protección de los datos de carácter personal en el ámbito sanitario. Usos de la historia clínica”, en GARRIGA DOMINGUEZ, Ana y ÁLVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos personales, especial referencia al registro obligatorio de los portadores del VIH, Dykinson S.L. 2011, p. 11. la autora resalta la diferencia expuesta por la sentencia del Tribunal Constitucional 192/2000 de 30 de noviembre, sobre la función y en consecuencia el objeto y contenido, entre el derecho fundamental a la intimidad y el derecho fundamental a la protección de datos, dado que el derecho fundamental a la intimidad tiene como función proteger frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar que la persona quiera excluir del conocimiento ajeno, por otro lado, 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 derecho del afectado.

En el caso de las enfermedades, por ejemplo, la información sobre aquellas transitorias y comunes son las de menor afectación, ya que es usual tenerlas y salir de ellas, sin mayores consecuencias, no es sorpresa para nadie, por ejemplo padecer de un resfriado común, pero no sucede lo mismo con las enfermedades terminales como el cáncer, éstas sí que generan distanciamiento en algunos casos y ni hablar de las contagiosas como el SIDA, que genera el rechazo y aislamiento del enfermo desde su aspecto laboral hasta el resto de su entorno social y familiar. Así, FERNÁNDEZ PROL señala que en cuanto a esta enfermedad supresora de la defensas, “la carencia de información precisa, los prejuicios y los temores determinan un trato peyorativo para seropositivos y enfermos de SIDA”¹³¹, a lo que ALVAREZ GONZÁLEZ agrega que dicho trato diferenciado produce un rechazo, no sólo por el padecimiento de la enfermedad, sino porque la misma también se asocia con comportamientos que ofenden los sentimientos y la sensibilidad moral de las personas, lo que provoca intolerancia, indignación y disgusto¹³². En resumen, es difícil hacer público un padecimiento, si tener una enfermedad implica una posible diferencia en el trato posterior, por eso es que existe tanto temor y recelo en develar este tipo de información.

Por eso es que el derecho a la confidencialidad de los datos de salud se hace tan importante, la respuesta ante ella no siempre es la más positiva, no es posible que se permita la divulgación abierta de las condiciones de un enfermo, que además de cargar con la debilidad propia de su falta de salud, además vería como su derecho a una vida tranquila estaría en riesgo. Por las razones antes expuestas, la LOPD 15/1999, deja claro que esta

¹³¹ FERNÁNDEZ PROL, Francisca, “Análisis de la discriminación por enfermedad en el ámbito laboral. Especial referencia al caso del SIDA, en GARRIGA DOMINGUEZ, Ana y ALVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos personales, especial referencia al registro obligatorio de los portadores del VIH, Dykinson S.L. 2011, p. 151

¹³² ALVAREZ GONZÁLEZ, Susana, Aspectos éticos y jurídicos de la comunicación de datos del paciente con VIH/SIDA a terceros interesados en la información, en GARRIGA DOMINGUEZ, Ana y ALVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos personales, especial referencia al registro obligatorio de los portadores del VIH, Dykinson S.L. 2011, p.156

información se considera sensible, del nivel más alto de protección, sujeta a múltiples procesos, con el fin de proteger a sus titulares. Esta característica la desarrollaremos en párrafos siguientes, pero conviene advertir desde ahora su importancia, y el impacto que tiene tanto para el enfermo como para su familiares.

Ya en capítulos anteriores hablamos sobre la confidencialidad y el secreto profesional, de la importancia de mantener en reserva esta información y cómo la ley prevé sanciones a quienes en uso de su formación profesional, develan, comparten o difunden esta información, sin los controles adecuados y sin el consentimiento del paciente. Sobre lo anterior, esta conservación de los datos se presenta con fuerza dentro de la protección del dato de salud, pues además se considera deber moral, ético, legal que tiene el médico (profesional) frente a su paciente, de allí que la ley penal no es ajena a esta realidad y ha tipificado esta conducta como ilegal y sujeta a sanciones por parte del Estado.

Por otro lado, en este trabajo reconocemos que mucho del avance científico y de remedios para la salud se ha logrado con el ensayo y el uso que se da a los historiales clínicos, lo cual crea otra encrucijada para el derecho, ¿cuánto debe el enfermo reservar de su historial de salud?, si el avance médico y la sociedad en general podría depender del acceso a dicha información. Luego, entonces ¿cómo lograr que esta documentación, además de estar debidamente codificada y protegida ante terceros, se accesible sólo por aquellos que tengan derecho legítimo a ella?

Esto último si que nos lleva a la reflexión, pues un médico debe conocer “toda” la información del paciente para poder diagnosticar correctamente su padecimiento, pero al hacerlo somete al paciente al desprendimiento, por lo menos temporal, de múltiples facetas de su intimidad, tema que también abordamos ampliamente en capítulos anteriores. Sin embargo, ¿cuánta intimidad puede perder una persona a cambio de la salud?, la intimidad corporal parece la menos difícil de compartir, pues si se realiza con los controles básicos no

habría inconveniente, pero ¿qué sucede con la intimidad documental, aquella que perdura más allá de la simple consulta?, y que puede hacer mucho daño en manos equivocadas. O ¿qué pasa con el entorno familiar?, ya que parte del proceso de preguntas que generalmente realizan los profesionales de la salud al paciente, implican además preguntas del orden familiar, sobre los antecedentes de las enfermedades, e inclusive los padecimientos de padres, hermanos, hijos, entre otros.

El reto para esta difícil tarea la asume el derecho y sus reglamentos posteriores, temas que abordaremos en páginas siguientes. La verdad es que de todo esto es difícil concretar una división exacta de materias en el tema de salud, es algo muy complejo y abundante, las normas locales, estatales y comunitarias, van dando forma día a día al modo de interpretar este derecho tan importante, sin embargo, cada vez surgen más consultas sobre cómo actuar en casos concretos y cómo debe ajustarse la sociedad ante este nuevo derecho de sus ciudadanos.

3.1. Definición del dato de salud.

Los datos de salud son reconocidos por leyes nacionales e internacionales, como un “tipo” de información altamente sensible, dada su estrecha cercanía con la intimidad y dignidad de las personas, el propósito de esta clasificación es justificar que estos datos se puedan ocultar legalmente al público o a personas no autorizadas, porque su revelación ocasionaría un daño previsible a un interés protegido por el derecho, y que ha sido concedido a las personas. En este sentido el dato de salud se entrega en razón de la confianza que tiene el enfermo, en que todo lo dicho estará bajo el amparo del secreto, en consecuencia su revelación ilegal constituiría una grave infracción de la buena fe que se le demostró inicialmente. En si, estos datos sólo cabe recabarlos por razones de interés general cuando lo disponga una ley o el afectado lo consienta expresamente.

Esta condición especial hace inminente que tanto legisladores como jueces hayan reconocido la urgente necesidad de proteger la información que pueda describir un perfil de salud de las personas y que de este perfil “otros” puedan sacar ventajas oscuras, ajenas al derecho que tiene cada ciudadano. Tal como lo señala el Informe Jurídico 0600/2009, esta especial protección conferida a los datos relacionados con la salud de las personas no es arbitraria, sino que resulta de lo dispuesto en las normas Internacionales y Comunitarias reguladoras del tratamiento automatizado de datos de carácter personal. En este contexto, tanto el artículo 8 de la Directiva 95/46/CE, del PE y el CUE, así como el artículo 6 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección¹³³.

Para GÓMEZ SÁNCHEZ, los denominados datos de salud deben recibir una protección reforzada en todo caso, en razón de la información que revelan o pueden llegar a revelar y no en función del fin objeto del tratamiento de dichos datos¹³⁴. Esta autora reconoce que esta definición puede no ser de aplicación de manera general pero hace, una interpretación interesante al señalar que no todos los datos de salud efectivamente se refieren al tratamiento de las enfermedades que padecen las personas. A sensu contrario, existen otros objetivos que se pretenden alcanzar con la información que resulte de la condición física y mental del sujeto, lo cual coincidiría mucho con el avance y la tecnificación de nuestra época, así menciona casos como la investigación genética y lo importante de sus resultados para la resolución de casos policiales y hasta de prevención en la comisión de delitos. También, habría que decir que no todos los datos sensibles parecen estar al mismo

¹³³ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0600-2009, p. 1

¹³⁴ GÓMEZ SÁNCHEZ, Yolanda, “Comentario al artículo 7 – Datos de salud como datos especialmente protegidos”, en TRONCOSO REIGADA, Antonio (Dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas, 2010, p.648

“nivel” de protección, ya que también podrían existir categorías, atendiendo al contenido mismo, pues dependiendo del nivel de afectación del sujeto a la información podría diferenciar los niveles, inclusive entre datos del mismo paciente. Ahora bien un dato sobre el registro de ingreso al hospital no representaría tanta gravedad como aquellos que reflejen los medicamentos recetados, o peor aún los que se refieren a la patología que sufre el paciente, esta sería la idea general, aunque también debemos reconocer que la notoriedad del paciente, podría magnificar hasta el más sencillo de los datos.

En todo caso, tal como menciona la autora, mantener de forma inamovible esta “denominación restrictiva” a la información de salud puede provocar, a su criterio, gran dificultad a la hora de entender su real significado, lo que bien podría solucionarse si se permitieran clasificaciones “diferentes” a los datos de salud, a fin de maximizar las garantías que deben existir a la intimidad del individuo. No sé si esta solicitud de hacer una escalera en los tipos de datos de salud, sería la solución al conflicto por el uso plural de esta información, a lo mejor hacer una tabla general podría empantanar aun más el choque de derechos, pues nos parece que habría que analizar cada caso en particular, cada aspecto individual y salvaguardar en la mejor medida todos los intereses de las personas.

Sobre esto último, “no es fácil precisar, “a priori” y en abstracto, cuándo el desvelamiento de un dato personal o familiar produce perjuicio a una persona. Baste ahora con decir que lo produce siempre que se trata de un dato que el hombre medio de nuestra cultura considera “sensible” por ser inherente al ámbito de su intimidad más estricta, dicho de otro modo, un dato perteneciente al reducto de los que, normalmente, se pretende no trasciendan fuera de la esfera en que se desenvuelve la privacidad de la persona y de su núcleo familiar¹³⁵. La sentencia apunta, a nuestro criterio, a la consideración subjetiva del dato, pues lo que para unos es importante puede ser que para otros no tanto, así estaríamos

¹³⁵ STS, 234 – 1999, de 18 febrero, FJ: 2 (RJ 1999\510)

frente a la especialidad de los casos, atiendo a las diferencias que imprime cada persona a su propia realidad.

En el presente estudio, antes de entrar en el desarrollo de los instrumentos jurídicos que han sido aprobados para proteger los datos de salud, es imprescindible que primero se empiece por conocer ¿qué abarca dicho concepto? y; como no podría ser de otra forma, analizar la gran diversidad de acepciones que intentan definir ¿qué es un “dato de salud”?.

Alejados de interpretaciones subjetivas, en cuanto a su significado, nos vamos a referir directamente al derecho positivo vigente, cuya definición sobre el tema de salud es abundante y cuenta con múltiples propulsores, desde el aspecto internacional como el nacional.

3.2. Datos especialmente protegidos.

Proteger a las personas mediante la reserva de su información de salud no es tarea sencilla, para el Estado ha sido una larga tarea imponer el deber de apartar esta realidad del resto de las personas, apelando al buen sentido de quienes la poseen y el respeto a la privacidad que debe existir entre todos. Lo difícil es diferenciarlos del resto de datos personales, ÁLVAREZ HERNANDO señala que “no todos los datos tienen la misma importancia, por lo que no todos los datos concernientes a una persona son objetos del mismo nivel de protección, así por ejemplo, no es lo mismo que un responsable del fichero conozca la dirección de una persona que el dato sobre su tendencia sexual. Por ello, en buena lógica el legislador considera que existen determinados datos sensibles necesitados de

protección más cualificada, atendiendo a los potenciales riesgos sobrevenidos frente a un uso ilegítimo de esos datos”¹³⁶.

El concepto de datos sensibles (bajo el que se agrupan los datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos relativos a la salud y a la vida sexual y a condenas penales) han sido siempre problemáticos¹³⁷. Pero, contradictorios o no, esta categoría también responde a un avance en el pensamiento de la sociedad y de cómo nos vemos entre todos, lo que ahora se difunde es un tipo de derecho que hace 200 años nadie pensaba que existía o por lo menos no se le reconocía la importancia que hoy tiene.

Es por esto que reconocemos que el concepto de salud es tan amplio y su margen de vigencia tan extenso que pensar en una limitación exacta es en ocasiones es un tanto difícil, por eso es justo detenerse a analizar cómo queremos que sea la sociedad actual, más cuando se encuentra envuelta entre el gran desarrollo tecnológico y la obligación de conservar lo humano dentro del sector sanitario. De esta forma, hay que atender el tipo de protección que reciben los datos, conforme al modelo de gestión que se les aplique. Para ARTAL, Una de las características más importantes a tener en cuenta es “el gran volumen de información”¹³⁸ debido a la gran cantidad de datos que se recogen desde el momento que ingresa al paciente hasta su salida del hospital.

¹³⁶ ÁLVAREZ HERNANDO, Javier, Guía práctica sobre protección de datos, cuestiones y formularios, Lex Nova, 2011, p. 54

¹³⁷ RIPOL CARULLA, Santiago(ed.), Estudios de protección de datos de carácter personal en el ámbito de la Salud, Marcial Pons, 2006, p. 12

¹³⁸ ARTAL, Roser, “La informatización de los datos de Salud”, en RIPOL CARULLA, Santiago (ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Marcial Pons, 2006, pp. 105 – 119. Para el autor un elemento esencial a tomar en cuenta es la cantidad de información, sobre todo por el mantenimiento que requiere su custodia, además de la continua actualización que requieren dichos datos, pues no tener certeza de la novedad de los mismos haría su aportación mínima y casi nula.

La LOPD 15/1999, señala en su artículo 7, una serie de datos de carácter personal que tendrán un especial privilegio de protección, lo que se relaciona muy de cerca con el apartado uno y cuatro del artículo 18 de la Constitución Española, como hemos señalado en capítulos anteriores.

Los supuestos contemplados en este artículo son:

1. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente¹³⁹.

2. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

3. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Del mismo modo, los funcionarios administrativos, atendiendo al criterio de la gravedad o sensibilidad de los datos inscritos en la historia clínica, pueden acceder sin

¹³⁹ No obstante, la norma matiza y señala que podrán ser objeto de tratamiento los datos de carácter personal, 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. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

mayores resguardos a los datos vinculados a sus propias funciones, sin que esto suponga el acceso a toda la información del paciente, que igual podría ser protegida por la LOAP 41/2002 y la LOPD 15/1999. El ingreso al los expedientes clínicos por parte del funcionario administrativo tampoco escapa a la cobertura legal, por tanto, sólo sería justificando mientras se realice precisamente para cumplir con sus tareas regulares, cualquiera otra, fuera de sus funciones, si correspondería a un ingreso ilegal, luego entonces, sancionable.

Iniciamos con el análisis de ¿qué estar saludable? y ¿cuál es su alcance?, como respuesta tenemos que se considera saludable, al “estado en que el ser orgánico ejerce normalmente todas sus funciones”.¹⁴⁰ Por el contrario, su alcance ha sido progresivo y hemos pasado de sólo considerar el estado físico e incluimos además el estado psicológico. Lo que resulte como información sobre esta condición del sujeto, será conocido como dato de salud de una persona determinada. Ahora bien, aclaramos que nos referimos a los datos que se obtienen sobre las personas físicas cuyas características se encuentran enmarcadas dentro del género humano. Sobre la salud, la constitución Española remarca el derecho a la salud, y la obligación del Estado a velar por la misma, al expresar que “compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios. La ley establecerá los derechos y deberes de todos al respecto.”¹⁴¹

Asimismo, como se ha señalado en capítulos anteriores, la salud, no solo abarca el estado físico, y su vigencia no estaría tampoco determinada por el tiempo, si es un dato del pasado, del presente o del futuro, igual tendrá consecuencias, aún más los datos del futuro, pues en ocasiones determina si hay predisposición a alguna enfermedad, siendo los individuos aptos o no para una determinada situación. Para FERNÁNDEZ, en cuanto al estado de salud mental, “los datos psicológicos deben ser considerados a los efectos de la

¹⁴⁰ Definición por el Diccionario de la Real Academia de la Lengua Española

¹⁴¹ Constitución Española, artículo 43.2

aplicación de la LOPD 15/1999, como datos relativos a la salud de las personas. Para delimitar el fundamento de esta inclusión habrá de distinguirse entre los datos incorporados a historiales clínico – psiquiátricos o psicológicos¹⁴² y los no incorporados a los mismos¹⁴³.” Aquí el autor hace una diferencia, destacando que los primeros corresponden a los datos obtenidos mediante el tratamiento y que por su propia naturaleza son incluidos dentro de los historiales clínicos de las personas, y en cuanto a los segundos, se refiere a los datos que libremente aportan los pacientes o que forman parte de la apreciación del médico, los cuales no se han obtenido mediante tratamiento, sino por la plena voluntad del paciente de comentar o participarle su condición de salud.

Dentro del amplio aspecto de legislación autonómica, estatal y comunitaria, se aprobaron diversas definiciones que intentan desarrollar el concepto de salud, con algunas diferencias entre sí, algunas más amplias que las otras. Por ahora, menciono algunos de los más relevantes instrumentos jurídicos que protegen la información de salud.

3.3. Datos de salud del menor de edad.

La protección de los derechos de los datos de los menores de edad, ha sido ampliamente desarrollado por la legislación nacional e internacional, lo que facilita la protección de sus derechos, ante la posible violación por parte de terceros.

¹⁴² El informe psicológico clínico (IPC) es la comunicación (escrita u oral) confidencial y científica realizada por un Psicólogo a su cliente, representante legal o autoridad legal competente, de los resultados de un proceso de evaluación/intervención psicológica.

¹⁴³ FERNÁNDEZ LÓPEZ, Juan M., “El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario”, en Revista Derecho y Salud, Extraordinario XI Congreso Derecho y Salud, Volumen 11, Mayo 2003, p. 43

Así, la Convención de la Naciones Unidas sobre los derechos del niño (ratificada por España por Instrumento de 30 de noviembre de 1990¹⁴⁴), garantiza en su artículo 16, el derecho de los niños a la protección de la ley, contra las injerencias arbitrarias o ilegales en su vida privada. Igualmente, la Resolución del Parlamento Europeo, relativa a la Carta europea de los derechos del niño, establece en la Resolución A 3-0172/92 de 8 de julio, apartado 29, párrafo 8, que, “todo niño tiene derecho a no ser objeto por parte de un tercero de intrusiones injustificadas en su vida privada, en la de su familia, ni a sufrir atentados ilegales a su honor.

En ese mismo sentido, la Ley Orgánica 1/1982, de 5 de mayo, sobre protección del derecho al honor, a la intimidad y a la propia imagen, también precisa en su artículo 3, en cuanto a los menores de edad que su consentimiento deberá ser prestado por ellos mismos, si sus condiciones de madurez lo permiten y, de no ser así, el consentimiento habrá de otorgarse mediante escrito por sus representantes legales, quienes estarán obligados a poner en conocimiento previo del Ministerio Fiscal el consentimiento proyectado, habiendo de resolver el Juez si en el plazo de ocho días el Ministerio Fiscal se opusiere.

Ley Orgánica 1/1996, de 15 de enero¹⁴⁵, de Protección Jurídica del Menor, establece en su artículo 4.3 que “se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales”. Esta ley, que es desarrollo tanto del artículo 39.4 de la Constitución Española como de la Convención de los Derechos del Niño aprobada en las Naciones Unidas el 20 de noviembre de 1989, en vigor en España desde el 5 de enero de 1991, menciona en el artículo 11.2 como dos de los principios rectores de la actuación de los

¹⁴⁴ BOE número 313 de 31/12/1990, páginas 38897 a 38904 (8 páginas.)

¹⁴⁵ BOE núm. 15/1996, de 17 de enero de 1996

poderes públicos en su actuación de protección del menor, "la supremacía del interés del menor " y "la prevención de todas aquellas situaciones que puedan perjudicar su desarrollo personal", y dispone en el artículo 13.3 que en las actuaciones de protección "se evitará" toda interferencia innecesaria en la vida del menor ". Y en el artículo 17 de la misma Ley Orgánica se contiene el mandato de que "en las situaciones de riesgo de cualquier índole que perjudique el desarrollo personal y social del menor, la actuación de los poderes públicos deberá garantizar en todo caso los derechos que le asisten y se orientará a disminuir los factores de riesgo y dificultad social que inciden en la situación personal y social en que se encuentra"¹⁴⁶.

Ahora bien, en cuanto al derecho a conocer los datos de salud de los menores de edad, el tema tampoco ha sido pacífico, pues la LOAP 41/2002 establece a nuestro parecer, tres criterios definidos en cuando al acceso de los datos del menor de edad, así:

1) Mayor de 16 años hasta antes de los 18, plena capacidad para decidir sobre sus datos, y no cabe el consentimiento por representación (mayoría de edad sanitaria);

2) Mayor de 12 años hasta antes de de los 16, criterio de capacidad natural (madurez intelectual y emocional), presumiéndose la madurez¹⁴⁷ en los que han cumplido los 14 años;

¹⁴⁶ STS, 1251 - 2009 de 10 diciembre, FJ: 7 (RJ 2010\304)

¹⁴⁷ Cfr. En estos casos autores como ÁLVAREZ de NEYRA KAPPLER, Susana, "El consentimiento en la toma de muestras de ADN. Especial referencia a los procesos de menores (parte II), en Revista de Derecho y Genoma Humano, Universidad de Deusto, núm. 35, Julio – Diciembre, 2011, p.52, señala que operativamente sería conveniente que se obtuviera en todo caso la autorización judicial del juez de menores que le diera respaldo y cobertura a la obtención de la muestra del menor, dado que, si es aquél el que debe decidir el grado de madurez de cada menor afectado y siendo ese término (grado de madurez), un concepto jurídico indeterminado, los problemas que se podrían derivar de una errónea o, al menos discutible, calificación o consideración del mismo, quedarían directamente salvados, ofreciendo a su vez, una mayor eficacia y seguridad jurídica, que es lo que sin duda, proporcionaría esa autorización

3) Menores de 12 años, se requiere la conformidad de los padres o tutores.

En este sentido, el Informe Jurídico 0409 – 2004 señala que “si los padres de un mayor de catorce años acuden a un centro sanitario solicitando un informe de analítica o cualquier dato incorporado a la historia clínica de su hijo, sin constar autorización alguna de éste, no sería aplicable lo establecido en el artículo 18.2 de la LOAP 41/2002, por lo que no debería procederse a la entrega de la información en tanto no conste la autorización fehaciente del hijo. Por supuesto, salvo en los supuestos en que el hijo haya sido previamente sujeto a incapacitación”¹⁴⁸. De igual forma, aclara que en el resto de los menores de edad, no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162 1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez. Por último en los casos de pacientes, de 17 años de edad, tendría, salvo que se hubiese declarado su incapacitación, condiciones suficientes de madurez para ejercitar su derecho de acceso a la historia clínica, la entrega de datos existentes en la misma al titular de la patria potestad exigiría que previamente se hubiera conferido por la paciente la debida representación para ello, no bastando para entregar la información la mera aportación del libro de familia.

Por otra parte, el Real Decreto 1720/2007, que también regula esta materia, permite que el consentimiento pueda obtenerse de los menores de edad, que tengan como mínimo 14 años, pero advierte que no se puede utilizar a estos menores para obtener información de sus padres, tutores etc., dado que para estos casos deberá recabarse el consentimiento directamente de los titulares de la información. En este caso, el Real Decreto hace cuenta de esa “madurez”, que posiblemente muestre el menor, aunque en los casos de los pacientes menores de edad, deberá el médico encontrar mediana evidencia de

¹⁴⁸ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0409 – 2004, pp. 2 y 3

esta madurez, pues la LOAP 41/2002, permite sólo a los mayores de 16 años prestar consentimiento sin la presencia de sus padres.

También, debo señalar que entre los menores se cuenta aquellos que apenas han nacido¹⁴⁹, y cuya información de salud puede ser determinante para tomar decisiones durante el resto de la vida, como señala GÓMEZ CÓRDOBA, “en el ámbito clínico, los análisis genéticos realizados en la fase prenatal y postnatal (temprana o tardía), buscan determinar en general, las bases genéticas de las enfermedades, la susceptibilidad o protección a enfermedades, la respuesta a medicamentos, estilos de vida o sustancias tóxicas, el pronóstico o evolución de la historia natural de las enfermedades”¹⁵⁰. Esta autora también destaca la importancia de los datos de salud desde los primeros años, pues durante la fase postnatal temprana se accede a información genética a través de cribados en los recién nacidos para detectar tempranamente enfermedades de este origen o por sospecha de enfermedad genética o en casos de trastornos de la identidad sexual para determinar el sexo cromosómico mediante cariotipos. En definitiva, que estas informaciones serán fundamentales tomar decisiones cuando este menor llegue a la edad adulta.

Por esto, al igual que en los supuestos de información concerniente a los mayores de edad, los datos de salud de los menores, deben ser custodiados con los medios de seguridad establecidos por la ley, y no se puede mostrar la información de su historia clínica

¹⁴⁹ Aunque en este aspecto en el caso de las pruebas genéticas en gametos (óvulo o espermatozoide), en el ámbito de las TPAH, se podría usar para seleccionar donantes de la misma etnia, propender por la perpetuación de determinadas características fenotípicas, lo que podría considerarse eugenesia. Vid infra. GÓMEZ CÓRDOBA, Ana I., “Consentimiento informado para el tratamiento de la información genética en el Derecho Colombiano”.

¹⁵⁰ GÓMEZ CÓRDOBA, Ana I., “Consentimiento informado para el tratamiento de la información genética en el Derecho Colombiano”, en Revista de Derecho y Genoma Humano, Universidad de Deusto, núm. 35, Julio – Diciembre, 2011, p.188

a terceros¹⁵¹, mucho menos si con dicho acto, no se busca la cura del enfermo, sino la consecución de otros objetivos. Para conocer esta información, se deberá contar con el permiso de los padres, quienes tienen derecho a oponerse a su uso, aunque se divulguen por cualquier medio, sea escrito o electrónico¹⁵². Igualmente, este derecho no es total y pueden

¹⁵¹ STSJ Extremadura, 932 – 2002, de 25 noviembre, FJ: 3 (RJCA 2002\1184). En esta sentencia se determina que la parte demandada compartió información de la historia clínica de un menor de edad con terceros, sin el consentimiento de sus padres, con el objetivo de “tranquilizarse”, ante el proceso judicial en el que era parte. Personal, que no trató el problema médico del menor, conoció detalles de su estado de salud, bajo el consentimiento de la parte demandada.

¹⁵² En la SAN, de 20 octubre 2011, FJ: 7, 8 y 9 (JUR 2011\422804), la Audiencia Nacional, sanciona a una persona por colocar imágenes de unos menores de edad, en el portal informático Youtube, calificándolos como “los cerdos de pozuelo”, para esto la Audiencia nacional confirma una decisión previa dictada por la Agencia de Protección de Datos, con base a que hay “indicios” suficientes sobre la autoría del responsable, al probarse que para subir el video al Internet, se utilizó la cuenta telefónica del sancionado. En particular, tengo algunas dudas sobre la decisión, pues aunque se utilizó un router con capacidad para conectar un ordenador a la vez y efectivamente se hizo desde la cuenta telefónica del sancionado, esto a nuestro parecer no implica que justo dicha persona haya violentado el derecho a la protección de datos. Tal como él mismo explicó, a su vivienda acceden múltiples personas y cualquier ordenador pudo haberse conectado a dicho puerto, en el tiempo estimado de uso de la IP. Evidentemente podría responder por ser el dueño de la vivienda, pero no se esa condición lo hace ser el responsable del fichero, que en todo caso es a quien corresponde la sanción, además de la falta en el consentimiento para recabar los datos. Sobre el particular, es interesante el análisis que hace la SAP Valencia, 526 - 2006 de 6 septiembre, FJ: 2 (ARP 2007\34), cuando señala que “es la primera y principal garantía que el procedimiento penal otorga al ciudadano acusado frente al ejercicio en su contra de acciones penales y constituye un principio fundamental de la civilización, que tutela la inmunidad de los no culpables, pues en un Estado social y democrático de Derecho es esencial que los inocentes estén en todo caso protegidos frente a condenas infundadas, mientras que es suficiente que los culpables sean generalmente castigados, ya que la condena de un inocente representa una quiebra absoluta de los principios básicos de libertad, seguridad y justicia que fundamentan el contrato social y es por ello por lo que el derecho constitucional a la presunción de inocencia constituye el presupuesto básico de todas las demás garantías del proceso. Como regla del juicio, el principio de presunción de inocencia impone a la acusación la carga de la prueba por encima de cualquier duda razonable. Ello vincula al Tribunal sentenciador no sólo en el aspecto formal de la constatación de la

existir argumentos suficientes para mantener datos de un menor de edad, con las justificaciones legales.

Así, pasamos a detallar algunos casos en los que la obligación de contar el consentimiento de los padres, en el uso de los datos de sus hijos, ha sido tema de análisis por las autoridades judiciales.

La Audiencia Nacional¹⁵³ resolvió una controversia judicial, en el caso de un padre que pidió la cancelación de los datos de su menor hijo, inscritos en un fichero de la sección de menores de la Fiscalía de Madrid, solicitud que contó con opinión previa y favorable de la Agencia de Protección de Datos, pero que después no compartió esta alta autoridad judicial, ya que esta última consideró que las justificaciones planteadas por la Fiscalía¹⁵⁴, eran adecuadas para mantener vigente la información del menor de edad. El demandante, en nombre de su hijo, justificaba que dichos datos se habían incorporado a un fichero sin su autorización, lo que afectaba directamente los derechos de su menor hijo y en consecuencia ejecutaba los derechos de cancelación, toda vez que el perjuicio causado era grave.

En este aspecto policivo, se ha evaluado el conflicto de derecho que puede surgir por la toma de muestras biológicas para comprobar el grado de participación de un menor de edad, en la comisión de delitos, dado que se podría considerar como una vulneración al principio del interés superior del menor. Sobre el particular ALVARÉZ DE NEYRA, sostiene que “la anterior idea parte de un error de base, que acarrea consecuencias indeseadas, pues

existencia de prueba de cargo, sino también en el material de su valoración, imponiendo la absolución cuando la culpabilidad no haya quedado acreditada fuera de toda duda razonable”.

¹⁵³ SAN, de 9 octubre 2009, FJ: 6 (RJCA 2009\848)

¹⁵⁴ La Fiscalía contestó a la solicitud de cancelación mediante decreto de 21 de enero de 2008, en el que acuerda no haber lugar a la cancelación solicitada, por considerar que dichos datos no han dejado de ser necesarios para la finalidad para la que fueron recabados y registrados, pues su consulta será imprescindible en caso de que el menor (y hasta que cumpla la mayoría de edad) fuera nuevamente denunciado.

no puede haber un mecanismo de reacción de los poderes públicos si no se investiga el hecho y, por tanto, se carece de un indicio serio y racional para afirmar o excluir la participación del menor en aquél, de modo tal que el abanico de protección pública no se puede desplegar y, en consecuencia, tampoco puede proyectar sus efectos sobre el menor”¹⁵⁵. La autora explica además que el interés superior del menor es procurar la reinserción y la reeducación del mismo, que no se produciría si no se pudiera establecer su vinculación con el delito, no ya su autoría, que sólo sería posible afirmar tras el correspondiente proceso penal. Ante este análisis soy de la opinión que efectivamente no se puede confundir un principio de protección al menor, con la impunidad en la comisión de delitos, pero si es importante rescatar que en el caso de los menores de edad, las muestras biológicas y de perfil genético sirven no solamente para identificarlo, sino que también develan otros aspectos privados y de salud, que nada tendrían que ver con la investigación policial y que por tanto, deben ser excluidos del registro correspondiente a la investigación del delito. Asimismo, las muestras genéticas del menor deben servir para el caso que se le investiga en concreto y sólo cuando el menor tenga la categoría de imputado y en ningún caso debe ser el inicio de un fichero que lo estigmatice hacia el futuro, por la posible comisión de nuevos delitos, en los que se sospeche su participación.

En todo caso, también el propio sistema judicial, puede establecer medidas para salvaguardar los datos de un menor, para proteger su salud y hasta para asegurar las propias garantías del proceso. Así, la Audiencia Provincial de Barcelona señaló¹⁵⁶ que por encontrarse ante una persona menor de edad que tiene que testificar sobre hechos importantes presuntamente cometidos contra su persona. Además, tratarse de persona especialmente vulnerable, atendida la edad, la propia naturaleza del delito a enjuiciar y el dictamen del

¹⁵⁵ ÁLVAREZ de NEYRA KAPPLER, Susana, “El consentimiento en la toma de muestras de ADN. Especial referencia a los procesos de menores (parte II), en Revista de Derecho y Genoma Humano, Universidad de Deusto, núm. 35, Julio – Diciembre, 2011, p. 45

¹⁵⁶ AAP Barcelona, de 25 septiembre de 2002, FJ: 2 (ARP 2003\311)

médico forense, que dice que no es conveniente la presencia directa del acusado ante dicha persona menor, aconsejan de todo punto, para evitar riesgos relacionados con su integridad moral y psíquica, establecer las medidas de protección...¹⁵⁷, para impedir, tal como solicitó el Fiscal en un primer momento, el contacto directo entre menor y acusado.

Asimismo, aunque hemos señalado que existen excepciones al consentimiento, que igual podrían ser aplicables a los casos de los menores, por su misma condición, también habría que revisar el alcance de dicha excepción. Por ejemplo, abrir una cuenta bancaria, a nombre de un menor de edad, sin el consentimiento de los padres, bajo el supuesto del fomento de ahorro y la autorización de la ley, tampoco son excepciones del todo válidas. Así la Audiencia Nacional determinó que “respecto de la excepción a la necesidad de consentimiento inequívoco, para el tratamiento de datos personales de los menores, que se pretende sustentar ..., una cosa es que el Real Decreto-Ley 2532/1929, en relación con el Decreto de 14 de marzo de 1933, contemplan la tradicional actividad de fomento al ahorro infantil, y otra muy distinta que dichas normas permitan el tratamiento de los datos personales de menores de edad, a fin de abrir una cuenta corriente a los mismos, sin autorización y ni siquiera el conocimiento de sus padres o tutores, consentimiento cuya exigencia ha de ser especialmente calificada teniendo en cuenta las personas (menores) que han de prestar el mismo y que se regula, en la actualidad, en el artículo 13 del Real Decreto 1720/2007, de 27 de diciembre”¹⁵⁸. En este caso, no se discutía la posibilidad de la tenencia de una cuenta bancaria, pues “el hecho de que una persona sea menor de edad no significa, por ejemplo, que no pueda tener bienes y que como titular de dichos bienes pueda incurrir en una serie de responsabilidades y generar deudas de las que responder, aunque

¹⁵⁷ Buscando el equilibrio entre los derechos de la persona menor de edad y del propio acusado, derecho a la publicidad del juicio, se establecieron restricciones a la publicidad del juicio pero sólo para el momento de la declaración de la menor, impidiendo el contacto visual entre acusado y víctima.

¹⁵⁸ SAN, de 17 febrero de 2011, FJ: 3 (JUR 2011\77299)

eso si, tenga que actuar su representante legal por él”¹⁵⁹, lo que el tribunal analizó fue la obligación de poner en conocimiento de los padres, tal apertura de cuenta, a fin de que estuviesen advertidos de su existencia.

Algunas prerrogativas inclusive podrían tacharse como contradictorias con otros derechos, entrando en colisión con posibles derechos fundamentales, tal es el caso de la libertad de información (artículo 20.1.d CE). De allí que, cuando se trata, de la captación y difusión de fotografías de niños en medios de comunicación social, es preciso tener en cuenta, que el ordenamiento jurídico establece en estos supuestos una protección especial, en aras a proteger el interés superior del menor...¹⁶⁰. La determinación de estos límites debe efectuarse tomando en consideración la dimensión teleológica del derecho a la propia imagen, y por esta razón... debe salvaguardarse el interés de la persona en evitar la captación o difusión de su imagen sin su autorización o sin que existan circunstancias que legitimen esa

¹⁵⁹ SAN, de 29 junio 2005, FJ: 4 (JUR 2005\264576), Esta sentencia plantea que, lege ferenda, se pueda plantearse por el legislador si resulta o no conveniente la inclusión de los menores en los ficheros de morosos o si la protección de los derechos de los menores debería exigir cualquier otro medida especial, como puede ser la especificación que se trata de un menor y la edad , y la identificación de su representante legal, etc., para evitar que pudieran suscitarse casos en que se afectase a la salvaguardia de los derechos de los menores .

¹⁶⁰ STC, 158 – 2009, de 29 junio, FJ: 4, (RTC 2009\158) Esta sentencia resuelve el conflicto entre el derecho a la información de un periódico y el derecho a la propia imagen de un niño, considerando que se produjo una intromisión ilegítima en su derecho a la propia imagen del niño con la publicación de la fotografía que ilustra el reportaje toda vez que dicha fotografía, que identifica al menor como discapacitado (dato de salud), fue captada y difundida sin el consentimiento de los padres del menor, siendo por ello irrelevante que la entidad titular del centro (Apanda) en el que fue tomada la imagen prestara su autorización para ello. Asimismo, esta sentencia dijo que “ni existe un interés público en la captación o difusión de la fotografía que pueda considerarse constitucionalmente prevalente al interés superior de preservar la captación o difusión de las imágenes de los menores en los medios de comunicación, ni la veracidad de la información puede justificar esa intromisión ilegítima en el derecho a la propia imagen de los menores, pues este derecho fundamental del menor «viene a erigirse, por mor de lo dispuesto en el art. 20.4 CE, en límite infranqueable al ejercicio del derecho a comunicar libremente información veraz”.

intromisión. De ahí que hayamos sostenido que “la captación y difusión de la imagen del sujeto sólo será admisible cuando la propia y previa conducta de aquél o las circunstancias en las que se encuentre inmerso, justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que puedan colisionar con aquél¹⁶¹. En igual medida, “ha de partirse de la base de que siempre que no medie el consentimiento de los padres o representantes legales de los menores con la anuencia del Ministerio Fiscal, la difusión de cualquier imagen de éstos ha de ser reputada contraria al ordenamiento jurídico. A mayor abundamiento, aún en el supuesto de que se cuente con el beneplácito paterno o tutelar, si la imagen difundida atenta o menoscaba la honra, la intimidad personal y familiar y la imagen del menor, la utilización de la misma constituye un atentado al derecho a la imagen de su titular”¹⁶².

3.4. El dato de salud y las nuevas tecnologías.

Es un tema casi indiscutible, que el progreso que ofrecen los ordenadores ha revolucionado la forma como se tratan los pacientes a nivel mundial. En el campo médico igual se ha pretendido mecanizar y agilizar el trabajo humano para que éste sea más rápido, eficiente y seguro. Precisamente, sobre la seguridad y el secreto de la información, se tienen que hacer ajustes para mantener dichos datos en reserva, pues hay que partir de que este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, previamente analizada en este trabajo, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, relativos a la historia clínica de pacientes de varios centros de salud, no pueden ser conocidos por ninguna persona o entidad ajena al propio paciente y a los

¹⁶¹ STC, 99 – 1994, de 11 abril, FJ: 5 (RTC 1994\99)

¹⁶² STS, 1120 - 2008 de 19 noviembre, FJ: 2 (RJ 2008\6055). Esta sentencia también deja claro que cualquier colisión entre derechos fundamentales, debe ser tratada caso por caso, atendiendo a la adecuada ponderación de los intereses públicos y privados en juego.

médicos que le tratan y que, menos aún, puede circular libremente por Internet, pues en eso consiste precisamente el secreto¹⁶³.

En la actualidad, esta cuestión ha adquirido mayor importancia, porque se necesita tratar una gran cantidad de información de los pacientes casi en tiempo record, debido principalmente a la cantidad de enfermos que se le asignan a cada médico diariamente, sin contar con las emergencias que ingresan a los hospitales y que su comunicación posee una reglamentación propia¹⁶⁴. En fin que con cada paciente hay innumerables datos que se deben procesar para llegar a diagnosticar lo más correcto posible la enfermedad de la persona.

De la misma manera las computadoras, son máquinas capaces de almacenar y recobrar muchos datos a gran velocidad, lo que ayuda a agilizar el tratamiento o manejo de la información, que en ocasiones tomaría mucho tiempo al personal humano del hospital. Aunque las computadoras son un invento con menos de un siglo de creación, desde su aparición, su desarrollo y las aplicaciones de su uso, especialmente los de la salud han sido vertiginosos.

Los hospitales, por tomar un ejemplo, introducen mayor tecnificación a su servicio y cuentan a diario con nuevos modelos de ordenares más veloces y más fáciles de transportar, los que hace del trabajo médico un oficio más sencillo, más eficiente y más rápido. Actualmente, toda actuación sanitaria ha de considerar tres aspectos que son:

¹⁶³ SAN, de 11 febrero 2010, FJ: 3 (JUR 2010\67480)

¹⁶⁴ El número 112 como único número de urgencias europeo se adoptó por la Decisión de 21 de julio de 1991 del Consejo de las Comunidades Europeas (hoy de la Unión), con fines de facilitar el acceso a las urgencias.

resultados clínicos, satisfacción del enfermo y coste y en consecuencia la actividad sanitaria debe ser planificada y gestionada dentro de su entorno y con visión de futuro¹⁶⁵.

En todo caso, el manejo de la información, de forma oportuna es un factor decisivo en la medicina, sobre todo si dicha información se hace de forma integrada, más ahora que los trabajos médicos se hacen en equipos en los que varios profesionales atienden a una misma persona, por uno o varios males a la vez. Sin embargo, “la dificultad en la protección de los contenidos o informaciones que circulan por Internet es elevada, ante la popularización del uso de los medios informáticos, que ha posibilitado que la realización de actos ilícitos hayan tenido un aumento exponencial (sistemas, lenguajes, etc.)¹⁶⁶.

El médico tiene la difícil labor de articular la diversa información que ofrece el paciente y no sólo lo hace desde su perspectiva, también tiene la obligación de procesarla y hasta almacenarla para los otros colegas que igual que él que servirán de las mismas para llegar a los diagnósticos y tratamientos de la enfermedad. Sin embargo, que la medicina deba avanzar a través de la transmisión de conocimiento es irrefutable, pero debe compatibilizarse con una defensa estricta de la intimidad y del honor de las personas, que por problemática personal, son útiles al cuerpo médico. Si existe un interés científico, partiendo de que el contenido ataca tanto a la intimidad como al honor, afecta reputación y consideración personal, solamente deben tener acceso al conocimiento, los profesionales de la medicina, para ello las medidas de control sobre el material didáctico deben ser absolutas, cayendo responsabilidad primaria sobre la autoría¹⁶⁷.

¹⁶⁵ TOLOSA ASENJO, Miguel A., “Gestión hospitalaria y protección de datos médicos”, en RIPOL CARULLA, Santiago (ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Marcial Pons, 2006, p. 122

¹⁶⁶ MESSIA DE LA CERDA BALLESTEROS, Jesús A., La protección de datos de carácter personal en la telecomunicaciones, Universidad Rey Juan Carlos, Madrid, 2004, p.87

¹⁶⁷ SAP Vizcaya, 461 - 2000 de 18 mayo, FJ: 1 (AC 2000\3335) Esta sentencia señala a su vez que, aunque haya interés científico, no puede salir el conocimiento del profesional de la medicina, si hay un interés didáctico, uniendo sujetos pasivos del reportaje y zona de divulgación, debe impedirse el conocimiento de la identidad de

Aquí es que surge el valioso papel de la informatización de los datos de la salud, pues difícilmente se le puede exigir a un profesional de la medicina, y más en esta época, llevar físicamente todos los expedientes de sus pacientes, pues como es evidente, la historia clínica, más la papelería propia de la consulta, la recolección de datos o muestras con fines de investigación o los propios resultados, retan la capacidad al más prolijo despacho. Por estas características de la medicina, se van utilizando de forma cada vez más profusa, las ventajas de la informática y mientras más compleja es la especialidad médica, mayor disponibilidad y prestaciones deben tener el sistema de informática.

También es cierto que, la tecnología de la información afecta al modo como se atiende al paciente y sobre el proceso como se archiva y recuperan sus datos, la forma como se comparten datos de salud con otros especialistas y sobre finalidad del uso en si de tal información. El riesgo podría darse en la protección de los datos del paciente y de su verdadero control de acceso, pues aunque las nuevas aplicaciones informáticas de la medicina, como son las publicaciones electrónicas biomédicas, la telemedicina, impulsada por el auge de Internet y los registros informáticos de la historia clínica podrían mejorar la investigación de algunas enfermedades, no se puede arriesgar la confidencialidad de la información del paciente sin el debido control de otros usuarios.

Es casi obligatorio el hecho que los distintos profesionales y no profesionales que trabajan en un centro sanitario, o espacio en los que se presenten servicios de salud, estén vinculados al manejo de los expedientes de salud. Sobre este tema, su uso va desde el que presta el agente de salud, hasta el personal administrativo que apoya en el desarrollo de las

los mismos, el riesgo de vejar a un ciudadano es absolutamente elemental conforme a lógica. Con independencia del bien hacer, de su loable intención, de su aportación social, se ha cometido una grave negligencia, que ha producido un grave daño a la actora, los medios de control sobre reportaje médico, con sujeto pasivo de la comunidad, deben ser absolutos, sin preservación de identidad no pueden escapar a conocimiento del profesional, con fin didáctico solamente la imposibilidad de identificación da vía libre a la transmisión pública.

actividades del centro o espacio, claro que el modo de proceder en estos casos debe estar debidamente reglamentado, sobre los niveles de acceso y demás extremos, necesarios para garantizar la confidencialidad de la información, aunque esto no es del todo suficiente, ya que no basta con tener reglamentado estos aspectos, si el centro sanitario, por ejemplo, no garantiza que sus funcionarios cumplirán con las disposiciones establecidas para dicho fin.

Sobre lo anterior, al responsable del tratamiento de datos de salud debe exigírsele una diligencia específica para asegurar que dicho tratamiento cumple con los principios y garantías exigidos en la LOPD 15/1999, puesto que se constituye en un deudor de seguridad en materia de datos, y por tanto está en la obligación de dar una explicación adecuada y razonable de cómo protege la información accesible desde la Internet, siendo insuficiente con acreditar que adopta una serie de medidas para su uso, pues también es responsable de que las mismas se cumplan y se ejecuten con rigor.

De esta manera surge una necesaria relación entre las personas que están en búsqueda de un tratamiento de salud, y la Administración que está llamada a ofrecer o prestar sus servicios en pro de esta petición. Lo cierto es que, con base a esa información que suministra el paciente para lograr un correcto diagnóstico, se desprenden otros usos, los cuales ya hemos mencionado en capítulos anteriores, pero que, en este caso, se refieren a la planificación, acreditación, gestión y evaluación de sus propios servicios, lo que busca en el mejor de los casos, mejorar el trato que recibe el paciente.

Así las cosas, “se constata que en muchas ocasiones las cuestiones suscitadas se nos presentan bajo la forma de conflictos éticos, en los que los intereses en juego guardan relación con los derechos y obligaciones en relación con la información clínica, afecta a bienes y derechos que la Constitución reconoce como fundamentales, tales como la dignidad

de la persona, la vida e integridad física y moral o la intimidad”¹⁶⁸. Este trato a la información por parte de la Administración estará determinada por el modelo de atención que utiliza el Centro Sanitario, por ejemplo, que en ocasiones van desde la autonomía en el desarrollo de las tareas de planificación, financiación, compra y o provisión de recursos, hasta la descentralización de esos mismos servicios en otras instancias. De igual forma, dada la complejidad que conlleva cada uno de los aspectos aludidos es enorme¹⁶⁹, al hablar de información de salud, administrada por vía electrónica, es necesario que de cada intento de acceso al sistema se guarde, como mínimo, la identificación del profesional de que se trate, la fecha y hora en que se realizó, la parte de la historia clínica accedida y el tipo de acceso. Si el acceso es denegado por no cumplirse los criterios de acceso, esta denegación debe quedar también registrada.

Ahora bien, precisamente al hablar de servicios es correcto recordar, que a veces las instituciones sanitarias o sitios de atención de salud, ven desbordados la capacidad de atender el cúmulo y variedad de peticiones que se le presentan, por lo que se hace necesario establecer listas de espera, en las que se compilan diversos datos del paciente con el más puro fin de organizar la atención de sus requerimiento. En si, la principal herramienta que permite evitar, en la medida de lo posible, los riesgos derivados del uso fraudulento e indebido de los datos que afectan a la salud es la seguridad con la que se dote a las vías de comunicación que transportan esa información de especial importancia¹⁷⁰.

¹⁶⁸ AYERRA LASCANO, José M., “Regulación general de la historia clínica”, en Revista Derecho y Salud, Volumen 11, Número 1, Enero – Junio 2003, pp. 23 - 38

¹⁶⁹ BELTRAN AGUIRRE, Juan L., “Tratamientos de datos de salud en la prestación de servicios sociales”, en Revista Derecho y Salud, Volumen 18, número 1, Enero – Junio, 2009, p. 5

¹⁷⁰ MARTÍN DELPÓN, José Luis, “La protección de datos de carácter personal en el ámbito de las fuerzas armadas. La protección privilegiada de los datos relativos a la salud”, en Revista Española de Protección de Datos, Thomson, Nº 5, Julio – Diciembre -2008, p. 186.

3.5. Los datos de salud – genéticos.

El alcance del dato de salud, ha dado un giro copernicano con el desarrollo del genoma humano, pues ahora además de controlar el dato de salud físico (externo) y mental (interno), también hay que sumar el dato genético, que involucra no sólo al enfermo, sino a sus familiares, pasados, presentes y hasta los futuros.

Según comenta NICOLAS, estos datos genéticos tienen características muy relevantes, como son: “no dependen del sujeto, no varían a lo largo de la vida, son accesibles incluso tras el fallecimiento, acarrear igualmente peligro de estigmatización incluso previo a la enfermedad, suelen ser conservados durante largo periodo de tiempo en relación con el resto de los datos clínicos, son más propensos a brindar descubrimientos inesperados, son independientes de la edad del sujeto y del estado clínico del tejido humano y debido a su propia naturaleza son casi irrepetibles en otro ser humano, (entre otros)”¹⁷¹.

Del mismo modo, para ALVAREZ GONZÁLEZ, el genoma humano y la revelación de la información genética establecen un nuevo marco de referencia para el estudio de los derechos fundamentales¹⁷². Sobre el particular, la autora menciona la gran dificultad de la calificación de la información genética, basada en la naturaleza indeterminada y controvertida de este tipo de información, pero estoy seguro que dicha incertidumbre, se está perdiendo con los años, pues la tecnología sigue avanzando y a la vez que revela más información sobre los aspectos más profundos del ser humano, asimismo va aclarando aspectos necesarios para lograr la defensa legal de este tipo de información.

¹⁷¹ NICOLÁS, Pilar, “El concepto de dato médico y genético”, en RIPOL CARULLA, Santiago (ed.), Estudios de Protección de Datos de Carácter Personal en el Ámbito de la Salud, Marcial Pons, 2006, p. 88 y 89

¹⁷² ALVAREZ GONZÁLEZ, Susana, “El habeas data biosanitarios: especiales situaciones de conflicto en relación con los datos genéticos”, en GARRIGA DOMINGUEZ, Ana y ÁLVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos personales, especial referencia al registro obligatorio de los portadores del VIH, Dykinson S.L. 2011 p.51

Para JORQUI AZOFRA, “los peligros que pueden derivarse de un uso abusivo de la información genética entraña, en suma, limitaciones a la capacidad de los individuos para desarrollar en condiciones de igualdad y libertad, su actuación personal y social. De ahí que la realidad descrita nos permita vislumbrar la necesidad de proteger a los individuos a fin de que puedan construir y organizar su vida de relación con responsabilidad propia”.¹⁷³ La autora propone el respeto al derecho de la persona a consentir hasta dónde quiere participar en el análisis de sus datos genéticos, a la vez que defiende el derecho a determinar el conocimiento de los resultados y quién se puede servir de ellos, pero asimismo destaca que tales garantías están condicionadas a otros complementos indispensables, como son; la facultad de saber quién dispone de esos datos y a qué usos los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

Los avances científicos también sugieren la incorporación de nuevos modelos de atención, cuya relevancia encuentra base en el estudio de casos inusuales, para determinar protocolos de atención a futuro. Por lo que a mi respecta, esto ya es motivo de gran preocupación, pues el avance de la tecnología va horadando poco a poco los cimientos que aun existen sobre la intimidad y la protección de los datos, su impacto y agresividad son constantes para develar los datos de salud del paciente, puesto que ahora se puede elaborar la imagen genética de un sujeto, enfocado directamente en sus enfermedades, lo que puede resultar en la posibilidad de elaborar un catálogo de los individuos y hasta endilgarles características que aun no presentan, y que son mucho menos que evidentes o notorias.

¹⁷³ JORQUI AZOFRA, María, *Análisis genéticos en el ámbito asistencial: reflexión ético – jurídica*, Fundación BBVA, Edit. Comares, Granada, 2010, p. 220. En esta obra la autora reitera que los rasgos singulares de la información genética y los peligros que un uso inadecuado de la misma entraña para la identidad y dignidad humanas, así como para el disfrute de los valores de libertad, la igualdad y la intimidad, han alertado sobre la necesidad de reconocer especial relevancia al desarrollo jurídico de la protección de los datos genéticos personales.

Y es que dentro de los propios datos de salud, tal como lo hemos mencionado antes, puede que existan unos con mayor trascendencia que otros, o que afecten de una mayor forma al sujeto, debido a sus características individuales, lo cual no implica esencialmente una distinción permanente. Sobre lo anterior, los datos genéticos o de investigación biomédica deben contar con un consentimiento expreso y por escrito, ya que mediante este tipo de información, no solo se conoce la realidad de la salud de una persona, sino la pre disposición a ciertas enfermedades de toda su familia, lo que abriría aun más el campo de afectación por el uso de la información. Por tal motivo, “los datos que pueden obtenerse a través del análisis del ADN transparentan ámbitos extremadamente sensibles de la vida privada y de la propia realidad física de la persona, todo lo cual aconseja tratar con extrema prudencia y máximas garantías los datos de esta naturaleza, y adoptar medidas necesarias para tutelar los derechos fundamentales que pudieran verse comprometidos con estas técnicas”¹⁷⁴.

En efecto, la información genética del ADN, se utiliza ya con fines de identificación. Existe el riesgo del uso de la información genética a efectos laborales, etc. Asimismo, las técnicas de reproducción asistida, cuyo uso puede considerarse atención médica, en la medida en que constituyen un remedio a la esterilidad, pueden dar lugar a ficheros informatizados de datos sobre embriones humanos, que ofrecen una especial sensibilidad¹⁷⁵.

En este tema, el Informe Jurídico sobre tratamiento de datos genéticos para la localización de personas desaparecidas o en investigación criminal, emitido el año 2000, señaló que “prescindiendo de la discusión acerca de los efectos del análisis de ADN

¹⁷⁴ GÓMEZ SÁNCHEZ, Yolanda, “La protección de los datos genéticos: el derecho a la autodeterminación informativa”, en Revista Derecho y Salud, Volumen 16, XVI Congreso “Derecho y Salud”, 2001, p. 60

¹⁷⁵ HEREDERO HIGUERAS, Manuel, “La protección de datos de salud informatizados en la Ley Orgánica 5/1992, de 29 de Octubre, en Revista Derecho y Salud, Volumen 2, Número 1, Enero Junio, 1994, p.19

codificante o expresivo y no codificante, debe señalarse que, si bien es posible que del resultado del análisis de ADN no codificante no se deriven directamente datos de salud, dichos resultados vienen a conformar la huella genética de una persona, y por tanto, se encuentran íntimamente relacionados con su salud. Asimismo, cualquier dato personal de carácter genético deberá ser considerado como un dato que afecta a la salud de las personas y, por tanto, sujeto a las disposiciones específicas aprobadas para la regulación de este tipo de datos de carácter personal”¹⁷⁶.

Tal como lo menciona la Ley 14/2007¹⁷⁷, de 3 de julio, sobre Investigación Biomédica, preámbulo, “en pocos años ha cobrado enorme relevancia la obtención, utilización, almacenaje y cesión de las muestras biológicas con fines de diagnóstico y de investigación, son cada vez más frecuentes las investigaciones que implican procedimientos invasivos en seres humanos, y la investigación con gametos, embriones o células embrionarias se ha hecho imprescindible en el ámbito de la terapia celular y la medicina regenerativa. Sin embargo, estos avances científicos y los procedimientos y herramientas utilizados para alcanzarlos, generan importantes incertidumbres éticas y jurídicas que deben ser convenientemente reguladas, con el equilibrio y la prudencia que exige un tema tan complejo que afecta de manera tan directa a la identidad del ser humano”.

4. Obligación de disociar el dato salud.

Tal como hemos mencionado, el referente más común, en el que se pueden encontrar los datos de Salud, es el historial clínico/hospitalario, a nombre de pacientes o

¹⁷⁶ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico – Año 2000, p.2 Este informe jurídico señala que cualquier tratamiento que se refiera a los datos relacionados con la huella genética de la persona debe efectuarse con suma precisión y cautela, de forma que se respeten íntegramente las previsiones establecidas en la LOPD 15/1999 y la Recomendación (97) 5 del Comité de Ministros del Consejo de Europa, relativa a la protección de datos médicos.

¹⁷⁷ BOE número 159 de 4/7/2007, páginas 28826 a 28848 (23 páginas.)

enfermos que han acudido a dichos sitios, en busca de una cura a sus enfermedades, pero no todo dato de salud, se genera en un hospital ni por la investigación de una enfermedad, también pueden corresponder a características físicas o psicológicas evidentes en la persona, como el caso de la discapacidad. No obstante, existe un gran reto a resolver: hacer que los datos personales de salud, sean anónimos implica que hay que organizar o reorganizar muchas de las historias clínicas existentes, que en su mayoría, salvo claras excepciones, aun se mantienen en soporte físico. (Entiéndase en este aparte “el papel”). La dimensión del trabajo es enorme y el reto para los hospitales, por ejemplo, es grande, dado el gran interés que existe en proteger a las personas. En relación con esto también tenemos que decir que disociar los datos que ya existen implica la inversión de muchos recursos, tanto humanos como presupuestarios, lo que puede colocar esta obligación en una de las más difíciles de cumplir, si se entienden los complejos momentos económicos que generalmente viven los hospitales.

Disociar en todo caso es mantener en secreto la información, evitar que se conozcan a simple vista quienes son los dueños de dicha información (tipo de enfermedad, etc.), brindándoles la oportunidad de desarrollar sus vidas de forma regular, sin estar bajo el seguimiento de los demás. Asimismo, la anonimización es una obligación sine qua non para proceder al uso adecuado de la información o datos de salud, compilados en las historias clínicas del paciente, cuando el fin que se persiga sea la investigación científica, la docencia, etc. . Esta exigencia no sólo implica el uso de la información en los términos dictados por la ley, sino que a la vez debe tener como propósito buscar un mejor tratamiento o cura de la enfermedad. El uso de estos historiales clínicos, puede dar como resultado en nueva información, sobre las técnicas aplicadas en algunas enfermedades, los fármacos utilizados, o los efectos que causan en el enfermo. La realidad actual implica que esta información no debe perder su riqueza y valor científico, para así evitar repetir errores o desaciertos, cuyas consecuencias sería la pérdida de más vidas humanas o más daño a la salud de los ciudadanos.

Ahora bien, nos concentraremos en la información contenida en los historiales clínicos, y en las obligaciones que existen en el manejo de estos datos de salud, conforme al uso o destino que se le pretendan dar a los datos. Tal como lo expusimos en nuestro primer capítulo, la historia clínica puede tener múltiples propósitos, pero dentro de ellos, el más importante, es dejar constancia del tratamiento que ha recibido un paciente desde su ingreso al centro de atención (hospitales u otros), hasta su salida del mismo, atendiendo especialmente a la condiciones de ingreso y de salida.

La LGS 14/1986 y la LOAP 41/2002 vienen a desarrollar de manera muy clara las obligaciones y derechos que existen sobre la historia clínica, con el interés de aclarar aspectos importantes como son, documentos principales que debe contener, el acceso, propiedad y vigencia de la información lograda. Ya desde estas normas surge la obligación de proteger esta información de manera adecuada, cumpliendo estrictos controles para garantizar que sólo el personal vinculado a ésta, pueda conocer y utilizar los datos de un paciente.

A ello debo añadir que la LOAP 41/2002, establece que, en su artículo 17.1 y 17.6, que Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial. Asimismo, serán de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la LOPD 15/1999.

Surge entonces la obligación de conservar la información, pero con base a las condiciones que impone la LOPD 15/1999, que ha sido objeto de análisis durante todo este

trabajo. La LOAP 41/2002, impone una obligación aún más especial para los casos del dato de salud, pues en su artículo 16.3, reconoce que existen otros propósitos adicionales al uso de la historia clínica, como son: los fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, los cuales se regirán por lo dispuesto en la LOPD 15/1999, y en la LGS 14/1986 y demás normas de aplicación en cada caso.

En este mismo artículo dice, además, que el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial 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. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

En definitiva, la LOPD 15/1999, en su artículo 3, apartado f), señala que el procedimiento de disociación consistirá en todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. Esta obligación de mantener el dato disociado, para propósitos distintos a la atención de la salud del enfermo, corresponde a toda una evolución del derecho y al respeto a la dignidad de la persona enferma, no siendo posible que se pueda utilizar libremente su nombre y su padecimiento, para propósitos ajenos a su cura, o mejor dicho su uso debe estar condicionados a sistemas de seguridad y controles previamente determinados.

Es comprensible que con la incorporación de las nuevas tecnologías, y el alcance voraz de algunas redes sociales, la legislación internacional y en consecuencia la nacional hayan tenido que reforzar los controles en el uso de las historias clínicas y así evitar el cruce

innecesario de información sensible. Sobre esto último, surgen los problemas de controlar la información de salud contenida en papel físico y, aun más complicado, controlar la información que ya está disponible en versión digitalizada. El riesgo es tan alto que si alguna persona o grupo en particular logra robar información de salud¹⁷⁸, no disociada, puede perjudicar enormemente la moral de las personas afectadas.

En todo caso, la disociación implica separar de manera efectiva los datos de salud de los datos personales, aunque hay que reconocer que con base a las nuevas tecnologías, es casi imposible lograr una disociación total y sólo se podría considerar como “disociado” aquel dato que involucre esfuerzos desproporcionados para recuperar su vínculo con su titular. Sobre este aspecto, para una consulta específica, el Informe Jurídico 182/2004 de la Agencia de Protección de Datos ha señalado que la sola identificación de los datos con siglas no es del todo una anonimización pues aunque en la comunicación previamente realizada se identifiquen a los afectados por un código formado por las iniciales de su nombre y apellidos, la comunicación de los mismos a la Administración permitiría asociar los datos previamente facilitados con los datos identificativos de las personas, sin que ello implicase en ningún caso un esfuerzo desproporcionado, obteniéndose así un tratamiento de datos de carácter personal de personas completamente identificables¹⁷⁹.

¹⁷⁸ En una interpelación parlamentaria en la Asamblea de Madrid (enero – 2012), la diputada del Partido Socialista de Madrid, Carla Delgado, denunció que en un blog religioso, se dio la publicación de una lista con 22 nombres de pacientes transexuales operados en la unidad de identidad de género del Hospital La Paz, que depende de la Comunidad de Madrid, en dicho listado se adjuntaban generales (sin apellidos) y datos de los tratamientos recibidos. Los posibles afectados denunciaron que los datos, aunque parecían disociados, no lo estaban, pues eran perfectamente identificables las personas reales incluidas en dicho listado.

¹⁷⁹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 182-2004, p. 2. Este mismo informe considera que la drogodependencia de una persona, es un dato necesariamente asociado con su salud, por lo que la comunicación de los mismos debe cumplir los criterios establecidos por la LOPD 15/1999, para la categoría de datos sensibles, incluso en el supuesto de que el afectado no sufriera ningún tipo de dolencia.

4.1. El esfuerzo desproporcionado.

Pero ¿cómo debe darse esta disociación? Es suficiente con separar el nombre del paciente, de su tratamiento, con un código o número de identificación por ejemplo. La Agencia de Protección de Datos ya se pronunció sobre este tema, en su Informe Jurídico 0283/2008, y expone que, “para entender que se ha efectuado correctamente la disociación, es necesario que no se permita por ningún medio identificar al paciente”. Nótese que en su informe incluye la obligación de “por ningún medio”, lo que conlleva un alto nivel de compromiso con la protección y disociación de la información de salud.

En todo caso, tal como amplía la Agencia, es suficiente que exista la mera posibilidad, incluso remota, de que, mediante la utilización, con carácter previo, coetáneo o posterior de cualquier medio (proceso informático, programa, herramienta del sistema, etcétera), de acceder a la información concerniente a los pacientes y que mediante esta, se pueda revelar la identidad de los afectados, para que quede plenamente sometida a la LOPD 15/1999.

Por tanto, lo más correcto es exigir una disociación real y no disimulada, o por lo menos no adecuada, y que sólo se entienda disociado el dato de salud cuando se ha destruido el nexo con toda información que identifique al sujeto o cuando su recuperación implique esfuerzos desproporcionados, esfuerzos que pueden medirse en tiempo, trabajo, materiales requeridos, etc. Sobre este aspecto, este esfuerzo “desproporcionado” debe ser suficiente como para disuadir a quien intente obtener datos de salud de una persona en particular

Siendo de esta manera, lo más seguro es que un simple código numérico o literal no garantice realmente la disociación del dato de salud contenido en los historial clínicos, ni representaría un esfuerzo desproporcionado, ya que una correlación entre el número de

historia clínica asignado por el centro médico y la identidad del paciente “nombre y apellidos”, no parece en extremo laborioso.

En esto último, estamos totalmente de acuerdo con la Agencia de Protección de Datos, disociar un dato de salud es más complejo que sólo asignar un número, se requiere aislar cualquiera posibilidad de identificación de la persona.

4.2. La opinión del paciente para disociar el dato de salud.

En el tema de la disociación se ha analizado si existe obligación de comunicar tal procedimiento al paciente, antes de iniciar la anonimización de su información. En este tema lo más recomendable es comunicarle primero el procedimiento¹⁸⁰, a fin de que conozca el proceso de separación de su información del resto de datos que contiene el historial clínico, salvo que el propio paciente consienta que no se separe y se mantenga íntegramente toda la información.

Volvemos al consentimiento como base fundamental, con algunas excepciones y es que también hemos señalado que este derecho fundamental a la protección de los datos (salud), no es absoluto, y conforme a casos muy puntuales, debe ceder para permitir el ejercicio de otros derechos, siempre y cuando estos supuestos estén contemplados por ley y se realicen conforme al respeto de los contenidos de los derechos en conflicto.

¹⁸⁰ GÓMEZ PIQUERAS, Cristina, “Disociación/anonimización de los datos de salud”, en Revista Derecho y Salud, Volumen 18, Número 1, Enero – Junio 2009, pp. 48 y 49. Además, la propia Recomendación Nº R (97) 5, de 13 de febrero de 1997, en su principio, 12.3, señala que “sin perjuicio de lo dispuesto por la legislación interna debe permitirse a los profesionales sanitarios habilitados para realizar su propia investigación médica el uso de los datos médicos que tienen en la medida en que el sujeto afectado haya sido informado de esta posibilidad y no se haya opuesto”.

4.3. Obligación de disociar para investigación.

Para los casos de investigaciones, la Recomendación Nº R (97) 5, de 13 de febrero de 1997, del Consejo de Europa señala, en el principio 12, que “siempre que sea posible, los datos médicos usados para fines de investigación científica deben ser anónimos. Los profesionales y organizaciones científicas y las autoridades públicas deben promover el desarrollo de técnicas y procedimientos¹⁸¹ para asegurar el anonimato”. Esto será como norma general, pero igualmente señala que pueden existir condiciones excepcionales, en las que no se pueda disociar el dato, lo cual haría “imposible” la investigación, que debe tener “fines legítimos”.

Estas dos exigencias, aparejadas en una misma excepción, implican la rigurosidad para justificar la no disociación de los datos. En cuanto a la primera, entendemos que se hace imposible la investigación cuando no existan otros medios adecuados y con iguales garantías que permitan la realización del estudio, por lo que no queda otra opción que mantener el dato de salud vinculado a la persona o paciente. De igual forma, el concepto de fines legítimos lo asociamos con fines legales, aquellos que están permitidos por el derecho positivo y que en ninguna medida podrían convertirse en propósitos oscuros cuyos resultados sean en detrimento de la persona que aporta los datos o la sociedad en general. Sin embargo, para otros autores¹⁸², estos fines legítimos significarían la adecuación de los fines de este último a los fines del primero y, por tanto, a los fines que se manifestaron al afectado en el momento de la recogida de los datos.

¹⁸¹ Para lograr anonimizar el dato de salud, los expertos sugieren: eliminar o sustituir algunos nombres de personas (físicas o jurídicas), direcciones y demás información de contacto, números identificativos, apodos o cargos; Eliminar o sustituir algunos lugares mencionados (ciudades, barrios, regiones, instalaciones, monumentos, áreas naturales, etc.); Mantener otros nombres de entidades (personas, organizaciones o lugares) cuando aportan información relevante para el caso y no facilitan la identificación; En ocasiones es necesario también filtrar fechas o cantidades monetarias.

¹⁸² MESSIA DE LA CERDA BALLESTEROS, Jesús A., Op. Cit., p. 103

De cumplirse ambas cualidades, la propia Recomendación N° R (97) 5, de 13 de febrero de 1997, exige además que:

a. el titular de los datos haya dado su consentimiento informado para uno o más fines de investigación; o

b. otorguen el consentimiento el representante legal o la autoridad o persona u órgano previstos por la ley cuando el afectado sea una persona legalmente incapacitada e incapaz de una decisión libre, y la ley nacional no le permita actuar en su propia representación, siempre que este consentimiento se dé en el marco de un proyecto de investigación relacionado con la condición médica o la enfermedad del afectado; o

c. el órgano u órganos designados por la ley nacional hayan autorizado la revelación de los datos con el fin de llevar a cabo un proyecto de investigación médica relacionado con un interés público importante, pero sólo si:

i. el titular de los datos no se ha opuesto expresamente a la revelación; y

ii. a pesar de los esfuerzos razonables que se puedan adoptar, sería impracticable contactar con el titular de los datos para pedir su consentimiento; y

iii. el interés del proyecto de investigación justifica la autorización; o

d. la investigación científica está prevista por la ley y constituye una medida necesaria por razones de salud pública.

Sobre los casos excepcionales, para realizar los estudios epidemiológicos, se ha dispuesto los intercambios de información en los casos de enfermedades infecto contagiosas, de las cuales, si no se lleva un control adecuado, pudiese resultar en un peligro grave para la sociedad. En ese caso, se ahonda en el ámbito de la vigilancia epidemiológica, precisamente por la naturaleza de las enfermedades de que se trata, en cuyo sentido el artículo 33 del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica, establece la declaración obligatoria de esta patología (SIDA), una vez detectada por el profesional correspondiente; así, ese precepto establece que los médicos, tras el diagnóstico, procederán a la comunicación inmediata y obligatoria al Registro del SIDA de la comunidad autónoma, añadiendo el artículo 34 del mismo Real Decreto, que "se recogerán los datos individualizados de cada uno de los enfermos diagnosticados mediante protocolo específico"¹⁸³.

4.4. Obligación de disociar para casos Judiciales.

No podemos olvidar que, además de la cura de la enfermedad, también existe una relación de servicio entre el paciente y su médico/centro sanitario, actividad que en su desarrollo puede generar responsabilidades civiles o penales, de acuerdo a la buena o mala práctica realizada por los profesionales de la salud. Esta posible falla en la prestación del servicio puede generar la intervención judicial, siendo la historia clínica el elemento básico de investigación. Mediante el análisis de diferentes causas judiciales se puede delimitar la responsabilidad penal o civil del personal sanitario (enfermeras, instrumentistas quirúrgicos, anestesiólogos), del médico y hasta del propio personal administrativo, en casos cuya actuación se realice al margen del derecho que constituya per se, alguna falta o delito.

Mucho se ha discutido si al juez debe llegar una historia clínica íntegra, con los datos de salud del paciente completa, sin pasar previamente por el filtro de las anotaciones

¹⁸³ STSJ Galicia, 5 - 2008 de 16 enero, FJ: 4 (RJCA 2008\700)

subjetivas y la información que corresponde a terceros. Sobre este tema el Informe Jurídico 36/2004 del Agencia de Protección de Datos señala que, “con carácter general, siempre que una autoridad judicial considere necesaria la aportación de datos contenidos en una historia clínica, en los términos que el propio Órgano determine, será necesario aportar dichos documentos, pudiendo resultar la decisión de la entidad a que se solicitara la información de no facilitarla o facilitarla parcialmente, contraria a lo dispuesto en el artículo 118 de la Constitución, a cuyo tenor “es obligado cumplir las sentencias y demás resoluciones firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos en el curso del proceso y en la ejecución de lo resuelto¹⁸⁴”

En este aspecto, soy de la opinión que el juez debe conocer la información completa, con todos los datos de salud, a fin de que pueda emitir su sentencia en forma adecuada. Tal potestad se basa en la solemnidad de los procesos, en los que se estima que la intervención judicial debe brindar la oportunidad tanto al demandado como demandante de utilizar todas las herramientas legales que considere necesarias para defender su causa. De igual forma, para verificar los procedimientos aplicados en el tratamiento curativo, lo más normal es que el juez solicite la historia de atención al paciente completa, y así hacer un recorrido sobre las etapas o tratamientos aplicados. Esta es la razón más importante para solicitar dicho documento, razón por la cual el juez puede determinar en ciertos casos si la información que debe revisar se debe mantener íntegra, sin necesidad de disociarse, para poder llegar a la verdad material del proceso.

De esto en particular, la LOPD 15/1999, debe ser aplicada con gran cautela, y en la medida en que resulte compatible con las funciones propias (jurisdiccionales y no jurisdiccionales) de los referidos órganos judiciales, pues la singularidad de la actividad jurisdiccional y los intereses que en ella subyacen, exigen en ocasiones una limitación o modulación de los derechos y garantías de los ciudadanos. La Audiencia Nacional también ha

¹⁸⁴ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 36-2004, p. 2

señalado que además de que el sometimiento de los ficheros judiciales a la LOPD 15/1999, ha de “entenderse sin menoscabo de la función jurisdiccional y, por tanto, atinente a lo que debe considerarse como "aspecto accesorio" o administrativo de la función jurisdiccional, centrándonos concretamente en el procedimiento judicial, existen también en él una serie de intereses y garantías que ostentan un trascendente valor en dicho proceso, tales como el del verdadero esclarecimiento de los hechos o el legítimo ejercicio del derecho de defensa de las partes, que han de ser ponderados en aquellos casos en que dichos intereses y garantías confluyen con el derecho contemplado en el artículo 18.4 CE , hasta el punto de que pueden llegar a implicar una importante limitación de tal derecho de protección de datos personales”¹⁸⁵. Esto se suma a que, es una “excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien inicialmente no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones”¹⁸⁶”

4.5. Obligación de disociar para docencia.

En materia de datos de salud, también será necesario disociar esta información cuando su fin sea promover la docencia en la carrera de medicina impartida en las universidades, los colegios profesionales, las escuelas de enfermería o las escuelas de salud pública. En cuanto a la docencia, los usuarios directos serán los estudiantes y los docentes; éstos últimos podrán registrar la experiencia docente/profesional lograda en la atención del enfermo, lo que, a su vez, les permitirá proveer nuevos elementos en el desarrollo de las clases, al contar con más herramientas para la enseñanza de los estudiantes de ciencias de la salud.

¹⁸⁵ SAN, de 9 octubre 2009, FJ: 5 (RJCA 2009\848)

¹⁸⁶ SAN, de 22 octubre 2010, FJ: 3 (JUR 2010\382932)

Aunque la ventaja inmediata para los alumnos es conocer de primera mano experiencias y patologías reales, esto no es óbice para que se pueda utilizar la información total de los historiales clínicos. En todo caso debe diferenciarse entre los tratamientos y procedimientos aplicados al enfermo y sus datos generales. Aquí igualmente aplica el consentimiento previo e informado para el paciente antes de utilizar su caso para la docencia, salvo que se pueda disociar totalmente los datos de salud y hacerlos totalmente anónimos, lo que haga casi imposible que se pueda identificar quién sufría tal o cual dolencia, objeto de la investigación /docencia.

Por último, también hay que decir que ha sido motivo de duda definir qué dato debe permanecer anónimo en la historia de salud del paciente, los datos nominales o los datos clínicos, siendo los primeros los generales de la persona y, los segundos, aquellos tratamientos aplicados al paciente. Más allá de cualquiera interpretación, soy del criterio que el paciente puede recibir un código para identificarse mientras permanezca en un centro de atención de salud o un código para identificar su enfermedad y eso no implica que tal condición represente una protección eficaz ante la opinión pública. Por el contrario, lo más importante a nuestro parecer es eliminar el nexo que une ambos datos, pues es allí que radica la afectación, de lo cual, conforme a cada uso posterior que se le dé a los historiales de salud, se puede ir ajustando la existencia de esta vinculación, ya que no es lo mismo usarlos para propósitos judiciales, que para temas estadísticos o de investigación docente.

5. El consentimiento para el uso de los datos de salud.

En capítulos anteriores hemos señalado cómo la normativa, autonómica, estatal y comunitaria, prevé formas adecuadas para el uso de la información de salud, siendo el consentimiento uno de los temas más importantes, pues toma en cuenta al titular de la información, previo a acceder a sus datos. Esto es así, pues al ser un tema confidencial e íntimo está sujeto a la voluntad de la persona, la cual puede disponer libremente sobre cuál

será su uso o, en todo caso, oponerse a que dicha información sea utilizada sin controles. En este sentido, el Informe Jurídico 0194-2009 de la Agencia de Protección de Datos, señala que “la manifestación de los requisitos legalmente exigidos al consentimiento del afectado se realiza en la práctica a través de la información al afectado, en el momento de la recogida de sus datos de carácter personal, de los extremos esenciales relacionados con el tratamiento, recabando a tal efecto su consentimiento en relación con los aspectos específica e inequívocamente hechos constar en la mencionada información”¹⁸⁷.

Y es que la información puede considerarse como un bien del cual se puede sacar mucha ventaja si al identificar la singularidad y vulnerabilidad del enfermo, se le acosa con ofertas médicas, curativas y de múltiples fines, cuyo único propósito es sacar provecho de su debilidad o falta de guía, aunque aprovecharse de ese mal, además de inmoral, sea ilegal.

Otro aspecto importante para recabar la información de salud es el consentimiento y la forma de expresarse, la LOPD 15/1999 lo califica como libre¹⁸⁸, dejando por fuera cualquier tipo de coerción o coacción, no contemplada por la autoridad, y que implique una renuncia a derecho. La sola contravención a estos criterios implica la nulidad de lo actuado y la posibilidad de que la entidad protectora de los datos, estatal o autonómica, según sea el caso, pueda iniciar expediente disciplinario y, de corroborarse la violación, imponer las sanciones correspondientes al infractor. Para la Audiencia Nacional, se trata de una garantía fundamental (el consentimiento), legitimadora del régimen de protección establecido por la ley, en desarrollo del art. 18.4 de la Constitución, dada la notable incidencia que el tratamiento automatizado de datos tiene sobre el derecho a la privacidad en general, y que sólo encuentra, como excepciones al consentimiento del

¹⁸⁷ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0194-2009, p. 2

¹⁸⁸ Según la Real Academia de la Lengua Española, se considera libre cuando se tiene facultad para obrar o no obrar.

afectado, aquellos supuestos que, por lógicas razones de interés general, puedan ser establecidos por una norma de rango de ley¹⁸⁹.

Se exige así, pues en el Informe Jurídico 11/2007 de la Agencia de Protección de Datos se señala que, no solo se debe lograr el consentimiento del afectado, sino que el mismo debe ser expreso. Por supuesto, reunir los requisitos generales que para la validez del mismo impone el artículo 5.1 de la LOPD 15/1999, es decir, que esté precedido de información suficiente que permita al interesado conocer la finalidad a que se destinarán los datos cuya comunicación autoriza y el tipo de actividad de aquél a quien se pretenden comunicar¹⁹⁰.

Pero, ¿cuándo debe obtenerse este consentimiento?, En principio debe ser antes de proceder a recoger los datos o, en su defecto, cederlos o comunicarlos a terceros, pues si no se cumple de esta manera o no se brinda esta facilidad “oportunamente” al interesado, podría dar lugar a la nulidad de documentación posterior que intente sanear dicha ausencia. Lo cierto es que la prestación del consentimiento para la cesión o comunicación de datos personales, y en mayor medida cuando se trata de datos de salud especialmente protegidos (art. 7 y 8 de la LOPD 15/1999), ha de ser, además de inequívoca y expresa, también previa, según el tenor literal del propio artículo 11.1 de la LOPD 15/1999¹⁹¹.

También es importante señalar que, para solicitar el consentimiento, se deben explicar todos los fines que se dará a la información recabada, por lo que pedir permiso por una causa, y después aparejada a ésta, dar otros usos a la información, no se encuentra dentro del amparo del consentimiento exigido por la ley. Siendo así que también es regla general la exigencia del consentimiento inequívoco del afectado para el tratamiento de datos

¹⁸⁹ SAN, de 23 noviembre 2006, FJ: 3 (RJCA 2006\902)

¹⁹⁰ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 11-2007, p. 2

¹⁹¹ SAN, de 8 de octubre de 2008, FJ: 4 (JUR 2008\336710)

de carácter personal (artículo 6.1. de la LOPD 15/1999), y sabemos que el legislador ha querido reforzar esta exigencia cuando se trata de datos especialmente protegidos (artículo 7.2 y 7.3), las excepciones a dicha norma general, como la prevista en el artículo 7.6, deben ser interpretadas de modo estricto sin que quepa admitir otros casos de dispensa del consentimiento distintos al que aparece expresamente contemplado en la norma¹⁹². La Audiencia Nacional señaló el error cometido por una empresa, en sólo pedir al trabajador, su consentimiento para registrar sus datos de salud en un fichero automatizado, pero no explicarle que una de las finalidades de ese fichero era posibilitar el ejercicio de control del absentismo laboral, que asiste a su empleador. Esa falta de acreditación de dicho consentimiento en los términos expuestos (inequívoco y expreso), no pudo ser suplida por conjeturas o informaciones genéricas a los trabajadores, que además no concretaban que sus datos se iban a incluir en un fichero de esas específicas características.

De igual forma, la sola aceptación de la persona no implica de inmediato que se pueda proceder con la utilización de los datos de salud. La LOPD 15/1999, en su ánimo de aclarar lo que corresponde a estos temas, contempla en el artículo 5.1, el deber de informar previamente al paciente, sobre los usos que se le dará a su información, quién la tendrá, qué recursos posee sobre los mismos y cómo utilizarlos. Su base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita. Sus contornos, por otro lado, se refuerzan singularmente en los denominados datos sensibles, como pueden ser, de una parte, la ideología o creencias religiosas, cuya privacidad está expresamente garantizada por la Constitución, en su art. 16.2; y, de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado; y los segundos, sólo serán susceptibles de recopilación

¹⁹² SAN, de 2 marzo de 2006, FJ: 6 (JUR 2006\118599)

mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia LOPD 15/1999 ha de fundarse en razones de interés general¹⁹³.

No puede confundirse este consentimiento informado para el uso de los datos de salud, con el consentimiento informado para el tratamiento médico, pues ambos tienen propósitos diferentes. El primero busca utilizar información, pasada, presente o futura para lograr un objetivo determinado o determinable; y, el segundo, sólo se refiere al conocimiento y aceptación de los riesgos que implica un determinado tratamiento médico, antes de ser practicado sobre el paciente. Es por esto que, como regla general, para tratamiento médico, el consentimiento puede ser verbal. Pero esto no es aplicable en el ámbito de la protección de datos, en el que se deben cumplir las formalidades que derivan de la LOPD 15/1999 y la LOAP 41/2002 que hablan de consentimiento expreso, lo que impide inducir dicho consentimiento en formas no concretas.

Evidentemente, la información que se ponga a disposición del interesado debe ser clara, sin mayores complejidades que las que exige la propia materia, dejando la certeza de que existe libertad para el sujeto en decidir si desea que su información sea utilizada. Aquí se puede poner en duda si los meros formularios con “relleno de casillas” cuentan como un consentimiento informado. Nos parece que no, pues la información podría variar conforme a cada caso, y en algunos temas debe ser más amplio que en otros. De allí que es obligación de quién solicita el consentimiento explicar con detalles el propósito de la recolección de información, quién la tendrá o compilará, a qué actividad desarrolla y demás derechos que tiene el dueño de tales datos. Esto no quita que se admitan las advertencias en los encabezados de páginas en algunos casos, sobre las finalidades de la recolección de los datos y los derechos que le asisten a las personas antes de entregar su información.

¹⁹³ STSJ Madrid, 757 – 2000, de 12 julio, FJ: 4 (JUR 2001\57391)

Uno de los elementos que más destaca la legislación, y que ha sido motivo de múltiples dictámenes judiciales, es la finalidad de la recolección de los datos, y su posterior uso. Sobre estos aspectos la LOPD 15/1999, en su artículo 5.1, señala que al solicitar el consentimiento se debe explicar con mucha claridad cuál es el fin que persigue la recolección del dato, el cual no podrá variar, sin el consentimiento previo del interesado. Tampoco su uso puede ser arbitrario. Siendo así, por más que se justifique haber logrado el consentimiento para el uso de un dato de salud, si éste se usa para otro diferente, no estará amparado en el consentimiento otorgado inicialmente. De igual forma, por ejemplo, ya desde la Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o persona se establecía que , “cualquiera que sea el modo de llevarse a efecto la recogida de datos de salud necesarios para la celebración del seguro de vida deberá constar expresamente el compromiso de la Entidad de crédito, de que los datos obtenidos a tal fin solamente serán utilizados por la entidad aseguradora”¹⁹⁴.

Esta información se debe dar al titular de los datos, como norma principal. Sólo en caso muy excepcionales a terceros, como es el caso de los padres, tutores o responsables y, si en todo caso, al tratarse de un paciente, su propia condición médica se lo impida.

5.1. Revocación del consentimiento: un derecho del paciente a decir no.

Así como hemos señalado que el consentimiento es un acto voluntario, sujeto a la decisión del afectado, debemos resaltar que igual le asiste derecho a cambiar de opinión, sobre el uso de información. Por tanto, el otorgar consentimiento no implica una obligación permanente e inmutable, para lo cual la LOPD 15/1999 y el propio Real Decreto 1720/2007 de 21 de diciembre, han establecido las condiciones necesarias.

¹⁹⁴ AGENCIA DE PROTECCIÓN DE DATOS, Instrucción 2/1995, de 4 de mayo, p.1

Si bien comienza la LOPD 15/1999, en su artículo 11, apartado 4, reconoce el derecho del titular, también la ley recoge la obligación del responsable del fichero al cumplimiento de dos elementos que consideramos fundamentales.

1. Establecer los medios, simples y sin mayor coste para el interesado, a fin de que pueda servirse de los mismos para comunicar su decisión de no continuar autorizando el uso de sus datos. La norma, prohíbe el excesivo formalismo y la burocracia, la tasación adicional y, en fin, los impedimentos que pueda sufrir el afectado para ejercitar su derecho.

2. Establece un plazo para que, de forma clara y sin lugar a dudas, se pueda conocer cuándo vence la oportunidad para el responsable del fichero de cancelar la información que tiene del paciente. En sí, el artículo 17. 2 del Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD 15/1999, dice que el responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la LOPD 15/1999.

El Real Decreto 1720/2007, en su artículo 32.2 señala además que la respuesta ante tales solicitudes debe ser expresa, por lo que entendemos que deberá existir una comunicación formal, dirigida al afectado en lo que se le ponga en conocimiento que se ha recibido su solicitud, el plazo que se ha utilizado para cumplir con su decisión y además, la diligencia de comunicación de esta revocación al consentimiento, en aquellos casos en los que se hayan cedido los datos, conforme al procedimiento exigido por la propia normativa.

No cumplir con este aspecto, igual podría ser objeto de investigación por la autoridad responsable, ya que se dejaría en indefensión al interesado, por no conocer si su

petición fue admitida y tramitada como corresponde, o si debe repetirla para lograr la anulación de sus datos de salud.

5.2. Excepciones al consentimiento en el uso del dato de salud.

Hemos dicho, casi hasta la saciedad, que el consentimiento es una exigencia fundamental, para el uso de sus datos de la persona y más en el caso de los datos de salud. También debemos reconocer que la propia LOPD 15/1999, y su reglamentación mediante Real Decreto 1720/2007, han establecido casos excepcionales, en los que puede exceptuarse este requisito y pasar directamente a recoger y ceder la información.

La propia LOPD 15/1999 establece excepciones en dos momentos y procesos diferentes, por un lado, en su artículo 6. 2, define las excepciones al consentimiento para “recoger” los datos, en cuyo caso destaca los siguientes casos:

1. Recoger datos para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias;
2. Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;
3. Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente ley;
4. Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Enlazado con lo anterior, la LOPD 15/1999 en su art. 11.2 habla de los datos que ya han sido recogidos y que procede a tratarse o cederse a un tercero. Dicha comunicación, también prevé situaciones excepcionales al consentimiento como:

A. Cuando la cesión está autorizada en una ley.

B. Cuando se trate de datos recogidos de fuentes accesibles al público.

C. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

D. 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.

E. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

F. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

En cuanto a que se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento, se ha planteado que en los supuestos de reconocimientos médicos¹⁹⁵, solicitados por el empleador, donde el paciente consienta al médico realizar las exploraciones necesarias, sólo puede conocer el empleador los resultados de los exámenes médicos, más no la patología que padece el trabajador. En sí, basta con conocer si es apto o no para el puesto, de ser el caso, pero en ningún momento debe conocer de otros detalles vinculados a su salud. En igual línea, la excepción sólo se estima cuando la instancia sanitaria presta servicios en busca de recuperar la salud del enfermo, situación que no sucede con los reconocimientos médicos, previa contratación, pues dichos facultativos realizan exploraciones al paciente no con el ánimo de curarlo, sino para generar un informe que después entregarán al empleador.

Dicho de esta manera, la Audiencia Nacional también ha dejado claro que las instituciones encargadas de hacer reconocimientos médicos a petición del empleador no están amparadas en la excepción de prestación de salud establecida en la ley. Específicamente expone que “no puede hablarse de prestación de servicios médicos en los términos exigidos en la ley, y ello aunque intervengan facultativos sometidos al secreto profesional, sino de otro tipo de prestación de servicios, no amparada en el art. 7.6 de la LPD, para cuyo tratamiento informatizado de datos se precisa el consentimiento del afectado”¹⁹⁶.

Y es que, en todo caso, como señala FERNÁNDEZ COSTALES, “la vigilancia de la salud realizada por estas empresas, tienen dos vertientes íntimamente unidas en esta

¹⁹⁵ El objetivo principal de esta vigilancia, basada en los reconocimientos médicos, es la de identificar posibles daños a la salud del trabajador, derivados del trabajo que realiza diariamente. En todo caso se busca definir cómo afectan las tareas asignadas al empleado, sus riesgos en su salud, además la manifestación de tales afectaciones al funcionamiento normal, físico y mental.

¹⁹⁶ SAN, de 23 noviembre 2006, FJ: 3 (RJCA 2006\902)

materia: la vigilancia de la salud, de carácter colectivo y la individual. Eso sí, aun cuando posee esta evidente vertiente colectiva, los conceptos regulados por la Ley de Prevención de Riesgos Laborales vienen a hacer referencia, fundamentalmente, a la vigilancia individual de la salud, y más en concreto a los reconocimientos médicos como una de las prestaciones sanitarias en materia de salud laboral¹⁹⁷.

Así las cosas, la Audiencia Nacional señala que cuando se trata de datos especialmente protegidos, como sucede con los referentes a la salud, la excepción a la regla del consentimiento en la cesión de datos únicamente se limita a cuando lo disponga una ley, «ex» artículo 7.3 de la ley, de manera que quedaría excluida el supuesto invocado relativo a la aceptación de un relación jurídica ..., pues, se trataría de una relación jurídica entre el titular del dato y la entidad¹⁹⁸, obviamente refiriéndose al centro médico que practica el examen y no otro.

Sobre lo anterior, aunque la comunicación dirigida a los jueces, también está dentro de los casos contemplados como excepcionales, no todo tipo de información dirigida a este sector se considera exenta de la obligación del consentimiento. Así ha quedado demostrado en un proceso disciplinario adelantado por “un juzgado”, a sus propios funcionarios, dentro del cual el titular utilizó información correspondiente a datos de salud del personal y los envió, sin consentimiento previo al superior, para comprobar el estado de desorganización en el que se encontraba dicho despacho. A la luz de este tema, la Audiencia Nacional señaló las diferencias que existen entre conocer un tema por asuntos judiciales y conocer de los datos por temas administrativos. Sobre este tema agregó, además, que no obstante, cuando el artículo 11.2 de la LOPD 15/1999 autoriza la cesión sin consentimiento

¹⁹⁷ FERNÁNDEZ COSTALES, Javier, “Intimidación de la persona y confidencialidad de datos en el marco de la vigilancia de la Salud. El respeto a los derechos del trabajador en los reconocimientos médicos”, en Revista Derecho y Salud, Volumen 16, número 1, enero – junio 2008, p. 82

¹⁹⁸ SAN, de 31 enero 2008, FJ: 4 (RJCA 2008\10)

de los datos reclamados por Jueces y Tribunales se está refiriendo a aquellos datos que están directamente relacionados con la función jurisdiccional, no a los datos, como ocurre en el caso presente, de que conoce un juez en ejercicio de una función de carácter netamente administrativa como es en relación a funciones disciplinarias y que fueron aportados a una denuncia en la Fiscalía y que carecía de ningún vínculo con los datos de salud que se aportaron a dicha denuncia ante la Fiscalía.¹⁹⁹

En particular, tal y como señala el Informe Jurídico 0471/2008 de la Agencia de Protección de Datos, no será necesario el consentimiento del interesado en la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.²⁰⁰”

5.2.1. Excepciones al consentimiento y uso de datos de salud del trabajador.

Como hemos señalado, el derecho a mantener nuestra información reservada no es absoluto y puede ceder en condiciones muy especiales, debidamente regulado por la ley. Pasamos a ver muy sucintamente el caso de los trabajadores y sus reconocimientos médicos, que también podríamos señalar como casos especiales. De acuerdo al Art. 22 de la Ley 31/1995²⁰¹ de 8 de noviembre, de Prevención de Riesgos Laborales, por regla general, todos los reconocimientos médicos deben realizarse, previo consentimiento del trabajador y bajo una clara información de los fines que se buscan. Sin embargo, ante esto también señala que se exceptuarán del consentimiento, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea

¹⁹⁹ SAN, de 20 febrero 2008, FJ: 5 (RJCA 2008\178)

²⁰⁰ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0471/2008, p. 3

²⁰¹ BOE 10 noviembre 1995, núm. 269, página 32590. (RCL\1995\3053)

imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

Del mismo modo, podría pensarse que, por interés público, es necesario conocer la realidad de salud de un trabajador, precisamente por las consecuencias que podría tener una baja en su desempeño o peor aún, poner en riesgo la vida o salud de terceros, si no se identifica con claridad, cuáles son sus capacidades para asumir sus tareas diarias. Para esto, la Ley 31/1995, de 8 de noviembre que Regula la Prevención de Riesgos Laborales señala, en su artículo 22 que el empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo. Pero dicha vigilancia se hará con el consentimiento del trabajador. En esta norma, además de regular la voluntariedad del sometimiento a las medidas de vigilancia de la salud y sus excepciones, se establece como criterio general que las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud²⁰². Luego entonces, los resultados de la vigilancia de la salud son los documentos que contienen los datos personales referidos a la salud del trabajador, derivados de la práctica de las diferentes pruebas a las que ha sido sometido para detectar el efecto que los riesgos de su puesto de trabajo provocan en su salud²⁰³.

²⁰² STS Asturias, 2760 – 2010, de 15 noviembre, FJ: 3 (AS 2011\129)

²⁰³ PEDROSA ALQUÉZAR, Sonia I., La vigilancia de la salud en el ámbito laboral, CES (Consejo Económico Social, Madrid), 2005, p. 121

Sobre este aspecto, el Tribunal Constitucional²⁰⁴ señaló que los reconocimientos médicos en la empresa no vulneran el derecho a la intimidad, cuando existen los siguientes requisitos: "la proporcionalidad al riesgo (por inexistencia de opciones alternativas de menor impacto en el núcleo de los derechos incididos); la indispensabilidad de las pruebas (por acreditarse ad casum la necesidad objetiva de su realización en atención al riesgo que se procura prevenir, así como los motivos que llevan al empresario a realizar la exploración médica a un trabajador singularmente considerado), y la presencia de un interés preponderante del grupo social o de la colectividad laboral o una situación de necesidad objetivable". De igual forma, conforme la configuración y finalidad del fundamental a la protección de los datos, los límites al mismo han de venir de la mano del ejercicio de los demás derechos fundamentales o del reconocimiento de bienes constitucionalmente protegidos, debiendo estarse a la regulación legal en cada caso, mediante una interpretación proporcionada en relación con los bienes jurídicos a salvaguardar.

Esta necesidad de la empresa de conocer el estado de salud de sus empleados también se encuentra fundamentada en el artículo 197.2 del Real Decreto 1/1994 de 20 de junio²⁰⁵, por el cual se aprueba la Ley General de la Seguridad Social. Este artículo señala que "el incumplimiento por parte de la empresa de la obligación de efectuar los reconocimientos médicos previos o periódicos la constituirá en responsable directa de todas las prestaciones que puedan derivarse, en tales casos, de enfermedad profesional, tanto si la empresa estuviera asociada a una Mutua de Accidentes de Trabajo y Enfermedades Profesionales, como si tuviera cubierta la protección de dicha contingencia en una entidad gestora". Siendo así, la empresa se ve obligada a proceder con los reconocimientos médicos a sus trabajadores, si quiere evitar la responsabilidad antes señaladas, gastos que tendría que cubrir y que no reembolsará la Seguridad Social, independientemente de las

²⁰⁴ STC, 196/2004 de 15 noviembre FJ: 6 (RTC 2004\196)

²⁰⁵ BOE 29 junio 1994, núm. 154, (página 20658)

responsabilidades aplicables en el ámbito sancionador administrativo, veamos algunos supuestos:

5.2.1.1. El reconocimiento para evaluar los efectos de las condiciones de trabajo sobre la salud.

Los avances e innovaciones en la mecanización del trabajo, los constantes cambios en los métodos de producción, las jornadas, las tecnologías, aptitudes personales, provocan una serie de condiciones que pueden afectar a la salud. Son las llamadas condiciones de trabajo, que se constituyen en un conjunto de variables que influyen en la realización de una asignación, en un área afectando la salud del trabajador en función de tres condiciones: física, psicológica y social.

Estas variables pueden crear una influencia tan directa que, en ocasiones, resulta imprescindible para el empleador conocer los efectos que dichas condiciones de trabajo crean sobre los trabajadores, un ejemplo de ellos pondría ser el estrés causado por el trabajo, ya que dicho padecimiento representa una amenaza para la salud de los trabajadores y, como consecuencia, a la salud de las organizaciones. Para que sea excepcional este reconocimiento de la salud, debe tratarse del único método posible, que no admita reemplazo, y debe realizarse de manera razonable, atendiendo a los propósitos iniciales. En este ejemplo podrían mencionarse las condiciones de alta tensión que se viven en las salas de urgencia de los hospitales, sumados a los cambios repentinos de horarios y la propia temática del trabajo, que implica tratar situaciones de dolor o tristeza y la necesidad humana de reponerse a la pérdida de seres queridos.

5.2.1.2. Reconocimiento para comprobar si el estado de salud del trabajador constituye un peligro para su integridad, la de sus compañeros o terceros.

Esta por demás señalar, que la excepción más clara la constituye la propia seguridad de los trabajadores, tanto individual como colectiva, la cual, como explica la LOPD 15/1999 y la Ley 31/1995 de 8 de noviembre, de Prevención de Riesgos Laborales, debe ser realizada a través de personal sanitario idóneo para ello y a través de técnicas de reconocimientos médicos específicos y contando también con la epidemiología laboral. Los reconocimientos médicos, como hemos visto en párrafos anteriores, deben ser acordes con los riesgos a los que están expuestos los trabajadores en cada uno de los centros de trabajo, porque es inadmisibile que se apliquen pruebas (entre ellas analíticas), que no se vinculen con las tareas que realiza el empleado. De allí, que la planificación y determinación de los factores de riesgo en un centro de trabajo deben realizarse con un equipo multidisciplinario, para poder detectar las enfermedades laborales o factores de riesgo de carácter laboral que existan.

Hay que ponderar el interés individual del trabajador, que de por sí es muy importante, con el interés del colectivo de sus compañeros de trabajo, y de los terceros que pudiesen compartir el espacio de trabajo. Sin embargo, para que esta excepción subsista, deben existir condiciones que realmente hagan suponer dichos riesgos, y no solamente sospechas sin fundamento. Un caso vinculado a este tema lo encontramos en el sector de la construcción, en el que las labores en conjunto exigen contar con todas las prevenciones y capacidades posibles, a fin de garantizar un trabajo seguro.

Del mismo modo, por ejemplo, en los casos del reconocimiento médico exigido al trabajador por posibles daños auditivos que le impedían realizar adecuadamente su trabajo. Sobre el particular la Sentencia 1657-2008 del Tribunal Superior de Justicia de Andalucía afirmó que la negativa reiterada a someterse al reconocimiento médico supuso un

incumplimiento grave y culpable de las órdenes empresariales, pues en este caso el trabajador se negó hasta seis veces a asistir al reconocimiento médico, sin embargo, aceptaba el dinero entregado por la empresa para el desplazamiento, por lo que la exigencia del reconocimiento no se consideró arbitraria, ni injustificada, ni tampoco es lesiva para el derecho fundamental a la intimidad al estar limitado este derecho por la obligación de la empresa a destinar al trabajador a un puesto adecuado a sus aptitudes físicas y a que no se encomienden al trabajador funciones que supongan un riesgo para sí o para terceros²⁰⁶.

5.2.1.3. Reconocimientos obligatorios por disposición legal.

Precisamente el Real Decreto 1/1994²⁰⁷, por el cual se aprueba el texto refundido de la Ley General de la Seguridad, establece en su artículo 196 que “todas las empresas que hayan de cubrir puestos de trabajo con riesgo de enfermedades profesionales están obligadas a practicar un reconocimiento médico previo a la admisión de los trabajadores que hayan de ocupar aquéllos y a realizar los reconocimientos periódicos que para cada tipo de enfermedad se establezcan en las normas que, al efecto, dictará el Ministerio de Trabajo y Seguridad Social”. Asimismo, la Ley Orgánica 3/1986, de 14 de abril²⁰⁸, de Medidas Especiales en Materia de Salud Pública, también prevé, en su artículo 2, que “las autoridades sanitarias competentes podrán 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 que se desarrolle una actividad”.

²⁰⁶ STSJ Andalucía, 1657 – 2008, de 12 mayo, FJ: 2 (AS 2009\964)

²⁰⁷ BOE 29 junio 1994, núm. 154, (página 20658)

²⁰⁸ BOE número 102 de 29/4/1986, (página 15207)

En principio, estas excepciones son válidas²⁰⁹, pero debe tomarse con sumo cuidado, pues el mismo Tribunal Constitucional ha dejado claro en otra sentencia²¹⁰ que el mismo interés público, acrecentado por el interés en preservar la salud (art. 43.1 CE) de aquél a quien se considera aquejado de una enfermedad que le impide desempeñar adecuadamente su trabajo y de los terceros con quienes deberá relacionarse en el curso de su actividad, puede justificar que la Administración Pública acceda a determinados datos de su historia clínica, si ese acceso se entiende imprescindible para poder preservar los intereses en conflicto. De esto hay que destacar la importancia de probar fehacientemente la existencia de dicho interés público pues, de no existir tal condición, se consideraría una intromisión ilegítima en la historia clínica de un paciente. No debemos olvidar que se trata de un derecho fundamental, protegido por la propia Constitución y que no puede, ni debe, ser anulado, bajo criterios espurios, sin contenido real o a espaldas del Derecho.

Sobre lo anterior, esta STC 70/2009 deja claro que aunque se pretenda justificar el acceso a una historia clínica bajo “supuesta” autorización legal, esta intromisión en los datos y la intimidad no debe dejar duda sobre su correcta interpretación, siendo imposible que se extienda la habilitación más allá de lo permitido por la norma. En si, dice que nada se establece en la norma aludida como justificante, acerca del modo en el que la Administración puede acceder a la información sobre el estado de salud del funcionario, y si alguna alusión al respecto se encuentra en el art. 7 del Real Decreto 172/1988, de 22 de febrero²¹¹, de procedimientos de jubilación y concesión de pensión de jubilación de los funcionarios civiles

²⁰⁹ Estas excepciones se justifican en que el derecho a la intimidad personal del artículo 18.1 y la autodeterminación en el uso los Datos 18.4 de la Constitución Española, no son derechos absolutos, sino que deben ceder "ante razones justificadas de interés general convenientemente previstas por la Ley, entre las que, sin duda, se encuentra la evitación y prevención de riesgos y peligros relacionados con la salud. Ese interés público es, desde luego, causa legítima que puede justificar la realización de reconocimientos médicos también en el marco de la relación laboral.

²¹⁰ STC 70-2009, de de 23 marzo, FJ: 5 (RTC 2009\70)

²¹¹ BOE. Boletín Oficial del Estado, 2 de Marzo de 1988 (núm. 0053)

del Estado, citado en el cuarto considerando de la sentencia, notorio es que esta mención de una norma sin rango de ley es, además de formalmente, materialmente insuficiente a los efectos requeridos de habilitación legal de la intromisión administrativa en la intimidad. Estamos convencidos que aquí el Tribunal hace una meridiana diferencia en cuanto a las justificaciones, tal vez atendiendo precisamente a esa diferencia en cuanto a lo especial de cada caso. Pues aunque se pretenda justificar el ingreso a los datos por mandato de ley, debe ésta última estar lo suficientemente justificada para lograr levantar el blindaje que se da a los derechos fundamentales.

El Informe Jurídico 0206-2010 de la Agencia de Protección de Datos, señala que, sin perjuicio de que el sometimiento a las acciones de vigilancia de la salud tenga, como regla general, carácter voluntario, quedando sujeto a la decisión y consentimiento del trabajador, es obligación del empresario poner a disposición del mismo la posibilidad de someterse a dichas acciones (obviamente también será obligación del trabajador someterse a aquéllas cuando ello no dependa de su consentimiento). Asimismo, destaca que las excepciones al consentimiento determinan las consecuencias en el alcance de la información a la que podrán tener acceso cada uno de los agentes involucrados en las acciones de vigilancia de la salud. Pero, al mismo tiempo, delimita los supuestos en los que la ley legitima el tratamiento de estos datos de salud sin contar con el consentimiento del interesado; es decir, los supuestos en los que el mencionado consentimiento quedará exceptuado por así preverlo una norma con rango suficiente²¹².

A contrario sensu, existen otros datos, vinculados a la salud, pero que no se constituyen en una afectación para la persona. Por ejemplo, la publicación en un tablón de anuncios sobre la baja de una trabajadora, pero que no dice el tipo de padecimiento que sufre, sólo explica su ausencia, no constituye una grave afectación en la moral del titular, al menos así lo entiende una sentencia del Tribunal Superior de Justicia de Aragón, “no se trata

²¹² AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico Nº 0206-2010, p. 3

de una exposición en el tablón de anuncios de la empresa de datos concretos sobre la salud de la trabajadora, sino únicamente sobre su situación de baja laboral por incapacidad temporal. Dato éste que no hace sino explicar la causa justificada de su inasistencia al puesto de trabajo y que no transciende o se entromete en el ámbito privado e indisponible para terceros de su intimidad ni de su dignidad personal”²¹³.

6. Índice de cumplimiento de la protección de datos de salud.

Para noviembre del año 2010, según informe elaborado por la Agencia de Protección de Datos (AEPD), sobre el Cumplimiento de la LOPD 15/1999 en los Hospitales, un tercio de los centros hospitalarios públicos españoles (35 por ciento) carecía de medidas para evitar la pérdida los historiales médicos o el acceso indebido a ello. Asimismo, el informe revela que el 30% de los centros públicos carece de las medidas para evitar la pérdida o acceso indebido a la documentación clínica durante su transporte. O que en el 35% de los hospitales el archivo de las historias clínicas carece de mecanismos que impidan su apertura.

De lo anterior, el informe señala que el cumplimiento de la normativa es alto en el conjunto de centros privados, alcanzándose niveles elevados en la mayoría de conceptos clave analizados: inscripción de ficheros (99%), inclusión de cláusulas informativas en los formularios de recogida de datos (94,5%), disponibilidad de procedimientos para atender el ejercicio de los derechos ARCO (97%) y, en general, en la implantación de medidas de seguridad y su auditoría periódica.

Por otro lado, cabe destacar que en el caso de los hospitales de titularidad pública, los indicadores varían significativamente según el aspecto y comunidad autónoma de que se trate. El informe parece reflejar mayor relajamiento por parte de los centros públicos, tal vez porque las consecuencias y las multas que se imponen las asume el Estado y

²¹³ STSJ Aragón, 540 - 2010, de 14 julio, FJ: 3 (AS 2011\249)

no los particulares que trabajan para éste. De lo anterior, una de las grandes críticas que se hacen es que la normativa actual no establece ninguna sanción económica para cualquier entidad pública que incumpla con la ley. En cambio, para los hospitales privados que incumplan la ley, existen multas de alrededor de los 600.000 euros.

Por otra parte, en los últimos dos años se ha constatado un incremento significativo en el número de las solicitudes de tutela de derecho relacionadas con el acceso a la historia clínica. En concreto, durante 2009 aumentaron las solicitudes a la AEPD para que tutelase el derecho de acceso al propio historial médico ante casos de entrega incompleta de la historia clínica personal amparándose los centros sanitarios en el derecho de los facultativos a la reserva de las anotaciones subjetivas en el historial del paciente; o denuncias de denegación de acceso al historial clínico de un familiar fallecido.

7. Resumen de ideas.

La investigación ha desarrollado el dato de salud de manera especial y centró su atención en algunos tipos de datos, como es el dato de salud de los menores y, dada la novedad que implican los datos genéticos, las consecuencias que existen por su obtención.

Precisamente por hablar de datos genéticos, esta investigación plantea un nuevo reto para el Derecho. Con la participación de las nuevas tecnologías queda en evidencia que los datos genéticos contienen información valiosa de salud de un particular, información que no sólo abarca su condición de salud actual, sino que incluso puede predecir dolencias o males que no se manifiestan de inmediato, sino que con el pasar del tiempo irán presentándose en el paciente.

Aunado a lo anterior, se deja sentado que el dato genético es de afectación amplia, por dar a conocer información del paciente y de sus familiares, lo cual agrega más

presión al derecho por reglamentar el uso de esta información y en especial la manera cómo se protege.

Por eso, la investigación incluyó la tarea de disociación, como una de las herramientas que la ley impone a la hora de utilizar cualquier tipo de dato de salud, cuyo fin es proteger en la mayor forma posible al titular de los datos.

El consentimiento también tuvo especial interés en este capítulo, pero se analizó el consentimiento para el uso de la información y no el consentimiento para tratamientos médicos, ya que son diferentes en contenido y propósitos.

Visto en su conjunto, los datos de salud se imponen con gran importancia ante el resto de los datos, pero interesa conocer en adelante uno de los ejemplos más típicos de organización de este tipo de información.

De allí que, en el próximo capítulo se analizará la historia clínica del paciente, por ser uno de los modelos más emblemáticos sobre el uso y custodia de este tipo de información. Sobre este dossier, la investigación analizará los propósitos para su elaboración y los múltiples usos que tiene, más allá de la atención curativa al enfermo.

Aunque es un compendio de información, comúnmente ubicado en hospitales, existe gran dificultad para determinar quién es su propietario, y tanto médicos, como pacientes reclaman los derechos que creen poseer sobre esta carpeta. Pero, ¿qué implica acumular este tipo de información? La respuesta inmediata sería la renuncia a parte de la privacidad o intimidad, pero ahora sabemos que no es solo eso, tener una historia clínica implica entregar no solo datos íntimos, sino datos personales, por lo que conviene conocer qué representa este documento y cuáles son sus características.

Con el ánimo de mejorar esta situación la LOAP 41/2002, desarrolló los elementos más esenciales de la historia clínica, aunque como veremos en el próximo capítulo, aun persiste el debate sobre el tipo de información que se puede entregar a cada uno de los interesados.

CAPITULO 3

LOS DATOS DE SALUD EN LA HISTORIA CLÍNICA

Sumario: 1. Aproximación al tema. 2. La historia clínica. 2.1. La regulación de la historia clínica. 2.2. Antecedentes jurídicos de la historia clínica. 2.3. Aprobación de la Ley Orgánica de Autonomía del Paciente (LOAP) 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. 2.4. Finalidad de la historia clínica. 2.5. Características de la historia clínica. 2.6. La titularidad en la historia clínica. 2.6.1. Del paciente. 2.6.2 Del médico. 2.6.3. De la Administración. 2.6.4. Posición ecléctica e integradora. 2.7. Acceso a la historia clínica. 2.7.1. Acceso a la historia clínica por el paciente. 2.7.2. Acceso a la historia clínica por el médico. 2.7.3. Acceso a la historia clínica por los familiares y terceros. 2.7.4. Acceso a la historia clínica por otros profesionales. 2.8. De la cancelación de datos en la historia clínica. 2.9. Conservación de la historia clínica. 2.10. La historia clínica informatizada. 2.11. Naturaleza jurídica de la historia clínica y su validez probatoria en procesos judiciales. 3. Resumen de ideas.

1. Aproximación al tema.

En el capítulo anterior vimos la importancia que tienen los datos de salud en la sociedad, la novedad del dato genético y la obligación de disociar la información de salud, antes de entregarla a terceros. En este sentido, el consentimiento tiene un papel importante para el recibo y la entrega de los datos de salud, en especial para determinar quiénes poseen la información y porqué pueden utilizarla.

Por tal motivo, se ha determinado continuar con un área muy especial dentro de este conglomerado de información. En adelante, este trabajo se interesa por los datos de la

salud depositados en la historia clínica, herramienta fundamental para el tratamiento de los pacientes, pero que, a la vez, brinda la posibilidad de hacer múltiples proyecciones aplicadas a diversas áreas.

En la mayoría de hospitales, la conservación de la historia clínica es responsabilidad del departamento de Documentación Médica quién se responsabiliza de su custodia, de dictar normas sobre el contenido y forma de realizar esta carpeta, así como de establecer las formas o controles para el acceso de los profesionales sanitarios a dicha información. En la mayoría de hospitales la conservación de las historias clínicas se realiza mediante un archivo central para todo el hospital, pero no implica que su uso sea exclusivo de los médicos, ya que existen otros profesionales y personal administrativo que tiene acceso a esta información sensible, siendo en ocasiones abierta a muchas personas durante el tratamiento de un paciente.

Este dossier de salud, con todos sus documentos, tiene carácter confidencial y privado. Siendo así, todos los profesionales que tienen acceso a dicha información en su actividad diaria tienen la obligación de mantener la confidencialidad. En caso de utilización de algunos de los datos de la historia clínica con fines docentes, epidemiológicos, etc., debe hacerse sin revelar ningún dato que pueda identificar al paciente, tal como vimos en el espacio dedicado a la disociación del dato de salud.

Los documentos de salud compilados en la historia clínica pueden ser muy variados y normalmente se clasifican en bloques de información. Así, toda la información que se genera de un paciente se almacena en grupos de documentos identificados con el nombre del paciente y su número de historia clínica, aunque esta clasificación no está del todo cerrada, pues permite que en la carpeta se puedan incorporar nuevos documentos, según la evolución del paciente y en sobre o sobres aparte aquellas pruebas diagnósticas de gran tamaño, tales como placas de radiografía y otros.

En vista de la importancia que representa para los datos de salud, la investigación continúa con el análisis de la historia clínica, su regulación y debate jurídico.

2. La historia clínica.

En los últimos años, la relación que existe entre el médico y el paciente ha cambiado radicalmente. La ciencia deja claro que el conocimiento no es estático y que los grandes avances en la cura de enfermedades también pueden, paralelamente, poner en riesgo los derechos básicos del ser humano.

Es un hecho fácilmente constatable que, durante las últimas décadas del siglo XX, las Ciencias Médicas han experimentado un avance vertiginoso. Pero no es menos cierto que cualquier hecho médico, tanto en el ámbito de la ciencia e investigación como el de la praxis clínica diaria, tiene inevitablemente un punto de referencia: el ser humano o si se prefiere, la persona humana²¹⁴.

Es así que la medicina moderna se ha racionalizado y especializado tanto que, en virtud de su conexión con las otras ciencias experimentales, ha modificado sus posibilidades prácticas de intervención en el trato de algunos dolores. Esta especialidad, apenas es necesario decirlo, constituye la solución dada por el ser humano a uno de sus principales problemas, el de ayudar al semejante cuando éste se haya enfermo²¹⁵. No obstante, la multiplicidad de factores y los cambios en el tratamiento del enfermo han despertado el interés del Derecho de regular el trato que se aplica a los pacientes, a fin de garantizar sus derechos fundamentales y normalizar la actuación de los profesionales de la salud.

²¹⁴ MARTÍNEZ MORÁN, Narciso, "Persona, dignidad humana e investigaciones médicas", en MARTÍNEZ MORÁN, Narciso (Coord.), *Bioteología, derecho y dignidad humana*, Edit. Comares, Granada, 2003, p.3

²¹⁵ LAIN ENTRALGO, Pedro, *La historia clínica*, consejo superior de investigaciones científicas, 1950, p.34

Ahora más que nunca, la responsabilidad por la salud del enfermo es bilateral, pues se obliga tanto a médicos como pacientes en la preservación de la salud, aunque existen nuevos derechos para el paciente, por ejemplo “la autonomía” que le permite tomar una “decisión aquí y ahora sobre un tratamiento médico que desea o le es propuesto en ese momento”²¹⁶. Además, existen obligaciones muy puntuales para el médico dada su labor profesional. De lo anterior, la investigación de este tema nos dice que la autonomía del paciente también debe balancear ese derecho reconocido por la ley, con los fundamentos de la práctica médica, puesto que sería muy complicado pedir a un profesional de la medicina que vaya en contra de sus propios principios, como es el de ayudar a curar al enfermo.

Así, en los casos de enfermos con desorden de identidad de la integridad corporal²¹⁷ sería muy difícil de tolerar su derecho a la autonomía en la elección del tratamiento médico, porque en estas situaciones, aunque esté informado de las

²¹⁶ LAPORTA SANMIGUEL, Francisco J., “Algunas incógnitas del principio de autonomía personal en tratamientos médicos, en MENDOZA BUERGO, Blanca (editora), Autonomía personal y decisiones médicas, Thomson Civitas, 2010, p. 21. En este aspecto LAPORTA señala que existen convicciones de fondo sobreentendidas, como es el caso de la búsqueda de la cura de la enfermedad, como presupuesto básico para asistir a consulta médica. Por tanto, si el doctor nos da indicaciones tendentes a lograr esa cura, debe entonces el paciente tener mucha justificación para no atender tales sugerencias y preferir oponer su derecho de autonomía ante tales prescripciones médicas. Demuestra así una posible inversión en la carga de la prueba, ya que el paciente deberá tener las razones que justifiquen su comportamiento. Así las cosas, pudiese existir un conflicto entre las reglas generadas por los principios de Bioética, el de autonomía y el beneficio (beneficencia) y, si priva el primero por el segundo, podría hablarse de un derecho a comportarse irracionalmente, independiente de las consecuencias que existan, algo así como Right to do wrong (derecho a hacer lo incorrecto).

²¹⁷ El desorden de identidad de la integridad corporal o BIID (sigla de Body Integrity Identity Disorder), es una enfermedad psiquiátrica que provoca en el individuo afectado un irresistible deseo por amputarse una o más extremidades sanas del cuerpo. A esta condición médica también se le conoce con el nombre de apotemnofilia y se da en individuos que no aceptan partes de su cuerpo o las rechazan por considerarlas extrañas, la mayoría de las veces piensan que con la amputación de dicha área su vida mejora notablemente.

consecuencias de mutilar su cuerpo, eso no lo libera de poner en riesgo su propio bienestar y el del profesional de la medicina que acepte realizar lo pedido por el enfermo.

Ante tal derecho a negarse y elegir el tratamiento, existe en la LOAP 41/2002 y los códigos deontológicos, la obligación del personal sanitario, y en especial a los médicos, de elaborar la “historia clínica del paciente”, como una regla sine qua non que les permite dejar constancia de las condiciones que presenta el usuario, antes, durante y después de recibir el tratamiento. Pues, aunque la ciencia médica no es exacta y el ejercicio de la medicina entraña riesgos²¹⁸, esto no implica que se no se pueda reglamentar lo actuado sobre el enfermo, en especial en defensa de sus derechos humanos. La recopilación de los datos obtenidos en el tratamiento del paciente constituye una de las misiones de importancia a desarrollar por el personal sanitario, así como su posterior plasmación en la documentación.²¹⁹

La historia clínica, en su concepto más general, es el conjunto de documentos en los que está contenida toda la información obtenida en los procesos asistenciales del paciente y tiene como fin principal facilitar la asistencia sanitaria, dejando evidencia de todos los datos que permitan el conocimiento veraz y actualizado del estado de salud del paciente. Este documento ha sido reconocido como el documento legal más importante, en cuanto a la relación médico paciente, ya que ahora se establecen mayores controles en el ejercicio de la medicina. De ahí que el Tribunal Supremo señale que en este documento debe quedar plenamente garantizado el derecho del enfermo a su intimidad personal y familiar y el deber

²¹⁸ RUIZ FEGER, Andrés, “Apuntes sobre la responsabilidad civil profesional en el sector sanitario”, en Revista Española de Seguros, Editorial Española de Seguros S.L., Enero- Junio, números 113 – 114, 2003, p.119

²¹⁹ ALONSO OLEA, Manuel y FANEGO CASTILLO, Fernando, Comentario a la ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, Edit. Thompson, 2003, p. 63

de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica²²⁰.

Para TIERNEY y HENDERSON, “los resultados de la historia clínica es el arte central de la atención del paciente”²²¹, refiriéndose a que debe existir una amplia relación de confianza entre el médico y el enfermo, con la suficiente oportunidad para encontrar los detalles y/o síntomas que identifiquen lo que actualmente aqueja al paciente. Sobre lo anterior, corresponde al médico²²² las obligaciones principales en cuanto al trato con el enfermo y no puede delegar en terceros no idóneos las funciones básicas, como la explicación del diagnóstico y la obtención del consentimiento informado²²³, previo a la intervención médica.

La práctica diaria en los centros de atención supone que este documento sea desarrollado mediante el método clínico, el cual incluye un proceso por etapas, a fin de llegar a un diagnóstico claro. Como pone de relieve la STS de 25 de octubre de 2002, el diagnóstico consiste en un juicio médico que precisa una fase previa constituida por una pluralidad de

²²⁰ STS, de 25 de febrero de 2002, FJ: 3 (RJ 2002/4107)

²²¹TIERNEY, Lawrence M Jr. / HENDERSON, Marck C., Historia clínica del paciente, método basado en evidencias, Edit. Mc Graw Hill, 2005, p. 3.

²²² STS, 1197-2007 de 23 de noviembre de 2007, FJ: 3 (RJ 2008\24)

²²³ La información requerida constituye un presupuesto y elemento esencial de la “lex artis” y como tal forma parte de toda actuación esencial hallándose incluido dentro de la obligación de medios asumida por el médico, de modo que la falta de información “no es irrelevante desde el punto de vista de la autonomía del individuo, puesto que se le priva de la facultad de decidir de acuerdo con sus propios intereses y preferencias entre las diversas actuaciones que pudiera considerar adecuada”. No obstante, excepcionalmente, no es preciso informar con detalles acerca de aquellos riesgos que no tienen un carácter típico por no producirse con frecuencia ni ser específicos del tratamiento aplicado, siempre que tengan carácter inusitado o no revistan una gravedad extraordinaria y, en este sentido, el art. 10.1 de la LOAP 41/2002 incluye hoy como información básica los riesgos o consecuencias seguras y relevantes, los riesgos personalizados, los riesgos típicos, los riesgos probables y las contraindicaciones.

actos, desde la anamnesis, a las pruebas de exploración física, radiológicas y analíticas, en definitiva, “un conjunto de actos médicos para iluminar y deducir la naturaleza de la afección que padece el enfermo”²²⁴.

En ocasiones nos encontramos con pérdidas de historiales clínicos, manipulación, negativa a su aportación, o manifestaciones del personal sanitario que no corresponden con el contenido del historial médico, extremos valorados muy negativamente por los jueces, y que sustentan condenas. De allí que GARCÍA HERNÁNDEZ señale que en la historia clínica se pone de manifiesto la competencia profesional, ya que no es un acto mecánico, sino un juicio clínico, puesto que se aporta formación, puesta al día, reflexión y supone un respeto del médico a los enfermos²²⁵. Es una máxima que los tratamientos y atenciones que no están en el historial, son difíciles de probar, o, dicho de otro modo, todo lo que no está en la historia clínica, se debe considerar como no realizado, siendo uno de los elementos probatorios a tener más en cuenta en la responsabilidad médica o sanitaria.²²⁶

Esta documentación del paciente es irremplazable para el Derecho por los criterios antes señalados, ya que abarcan desde la etapa de anamnesis o entrevista clínica, hasta la constancia del alta del paciente. Por ende, no se admite la pérdida de este documento, ni siquiera por culpa o descuido. Con esta idea, llama la atención lo expresado por el Tribunal Supremo²²⁷, cuando en la Sentencia de 23 de octubre de 2007, deja entrever que “la pérdida del expediente” formalmente aceptado por el hospital, “no ha impedido que se haya traído al proceso su contenido en la parte que resulta de trascendencia para la

²²⁴ SAP de Madrid, de 3 de marzo de 2003, FJ: 3 (JUR 2003\202913)

²²⁵ GARCÍA HERNÁNDEZ, Tomás, Manual del médico clínico para evitar demandas judiciales, Edit. La Ley – Actualidad. Madrid, 1999, p. 84

²²⁶ VAZQUEZ JIMÉNEZ, Francisco, “Aspectos prácticos de la responsabilidad médica”, en Revista Miramar, Revista del Ilustre Colegio de Abogados de Málaga, Noviembre/Diciembre, 2007, número 168, p. 53

²²⁷ STS, de 23 de octubre de 2007, FJ: 3 (RJ 2007\9373)

resolución del pleito”, pues este expediente puede ser remplazado con algunos documentos, que dan suficientes luces sobre el tratamiento prestado al paciente.

Esto resulta curioso, pues la historia clínica en principio, debe preservarse lo más completa posible, por ser responsabilidad del hospital su custodia y debe estar a disposición judicial de forma completa²²⁸, ya que contiene el sustratum de pruebas sobre la estancia y evolución del paciente en el hospital. Caso contrario, esta anormalidad demuestra qué tipo de cuidado y control administrativo se tuvo en dicho centro. La pérdida de este documento no puede tomarse como un elemento simple o accidental y, a criterio de esta investigación, debe ser valorado con gran profundidad en un proceso judicial. Recordemos que aunque la responsabilidad médica se rige por las reglas de la llamada “lex artis”, cuyo matiz culpabilístico es innegable, por el contrario, la responsabilidad sanitaria de los centros hospitalarios no sólo viene deducida de la llamada responsabilidad directa por hechos realizados por un tercero que le está subordinado, conforme al art. 1903 CC, sino también de la objetiva derivada de la Ley General para la Defensa de los Consumidores y Usuarios, cuyos arts. 1, 26 y 28 les son igualmente aplicables. Conforme al sistema de garantías y responsabilidad que establece su Capítulo VIII, el usuario tiene derecho a ser indemnizado de los daños y perjuicios demostrados, que la utilización de los servicios les irroguen salvo que dichos daños y perjuicios estén causados por su culpa exclusiva²²⁹.

Además, el derecho de acceso a la información clínica conlleva la obligatoriedad de los organismos públicos sanitarios de facilitar a los interesados sus propios historiales médicos en su integridad, para no ver limitado o coartado el derecho a la información sobre su estado de salud y los medios que se han dedicado a su reintegración y protección.

²²⁸ STS, 701-2000 de 25 de abril de 2000, FJ: 1 (RJ 2000\6096)

²²⁹ SAP, 225-2000 de Asturias, de 9 de mayo de 2000, FJ: 4 (AC 2000\1065)

Entender los preceptos citados de forma más restrictiva supondría dejar en manos de la Administración Sanitaria la información del propio estado de salud de los pacientes, sin posibilidad de acudir a otras vías que consideren humanamente más aconsejables, contrastando, o pudiendo fiscalizar, la labor que los propios servicios médicos efectúen con respecto a su propia salud, lo cual chocaría con el espíritu de las normas y la constitucionalidad de la que derivan.²³⁰

Sobre este tema, otro elemento importante sería la responsabilidad patrimonial de la Administración que se configura en el ordenamiento jurídico (art. 106.2 de la Constitución y 139 de la Ley Orgánica 30/1992), como una responsabilidad directa y objetiva, que obliga a aquella a indemnizar toda lesión que sufran los particulares en cualquiera de sus bienes o derechos, siempre que sea consecuencia del funcionamiento normal o anormal de los servicios públicos.

Si bien, no todo daño que produzca la Administración es indemnizable, sino tan solo los que merezcan la consideración de lesión, entendida, según la doctrina y jurisprudencia, como daño antijurídico, no porque la conducta de quien lo causa sea contraria a derecho, sino porque el perjudicado no tenga el deber jurídico de soportarlo (art. 141.1 de la Ley Orgánica 30/1992), por no existir causas de justificación que lo legitimen²³¹. Además, no todo diagnóstico equivocado provoca necesariamente responsabilidad médica, pues solamente se incurre en responsabilidad cuando se trata de un diagnóstico equivocado, interviniendo manifiesta negligencia examinado el caso concreto, o cuando no se han empleado los medios técnicos que ayudan a evitar los errores de apreciación²³².

²³⁰ STSJ, de 13 de diciembre de 1996, FJ: 3 (AS 1996\4139)

²³¹ STSJ, 208-2009 de Murcia de 13 de marzo, FJ: 3 (JUR 2009\332749)

²³² SAP, 57-2009 de Ávila, de 1º de abril de 2009, FJ: 4 (AC 2009\945)

En consecuencia, conforme al uso que se le imprima a este documento, la historia clínica posee múltiples funciones, bien desde el aspecto, ético, médico asistencial o jurídico, cada enfoque imprime mayor o mejor énfasis en su respectiva especialización. Sin embargo, nos mantendremos en el estudio jurídico, toda vez que interesa más para la elaboración del presente trabajo de investigación, aunque reconocemos el gran interés que representan los otros enfoques que se aplican a la historia clínica.

2.1. Regulación de la historia clínica.

En España, la regulación de la historia clínica está distribuida en tres grandes áreas: la primera es la ley Estatal, posteriormente, la ley o decreto que se apruebe en cada comunidad autónoma, en virtud del art. 148.21 de la C.E. y, por último, el reglamento o normativa particular que se realice a nivel de cada centro hospitalario. Todas estas regulaciones deben ser coherentes o complementarias entre sí, evitando las contradicciones con los principios rectores de la Constitución.

Como ley estatal tenemos a la LGS 14/1986²³³ que por mucho tiempo fue la principal norma que desarrolló los compromisos establecidos en el artículo 43 de la CE de 1978, entre ellos la obligatoriedad de elaborar una historia clínica por cada paciente de los centros asistenciales, lo cual sirvió de guía inicial, aunque un poco insuficiente, para mejorar el trabajo de los profesionales de la medicina, y el servicio prestado a los usuarios.

Con estos antecedentes quedó claro que era necesario adaptar el articulado de la LGS 14/1986 a la situación actual, dotando de un mayor contenido, de una mayor regulación a las relaciones médico – paciente, en lo que representa el tratamiento jurídico, facilitando el cumplimiento de la misma y garantizando, con ello, el desarrollo efectivo de los derechos

²³³ Publicada en el Boletín Oficial del Estado, número 101, de 29 de abril de 1986

que a los ciudadanos corresponde en este campo²³⁴. Como resultado a esta iniciativa de actualización normativa se aprobó la LOAP 41/2002, la cual tiene su origen en la proposición de Ley sobre Derechos de Información concernientes a la Salud y Autonomía del paciente y la documentación clínica presentada en el Senado por los grupos parlamentario Entesa Catalana de Progrés y Convergència i Unió y registrada el 29 de enero de 2001, siendo retirada el 21 de febrero de ese mismo año²³⁵.

Ambas leyes, tanto la LGS 14/1986, como la LOAP 41/2002, conciben al paciente como un ser completo en derechos y no como un conjunto de síntomas y dolencias. La aspiración de estas normas es cambiar el paradigma de atención, del enfoque paternalista al trato en derechos humanos. Ya con estos enfoques empieza el derecho positivo a modificar el rol de atención que desde antaño se venía desarrollando a nivel nacional. El modelo tradicional se había caracterizado por la relación directa entre el paciente y el médico. Sin embargo, hoy en día con gran frecuencia el tratamiento de un paciente requiere la participación activa, conjuntamente con los médicos, de un personal profesional muy variado²³⁶. En la mayoría de los casos, la atención médica del paciente es una labor de equipo. El paciente puede obtener grandes beneficios de tal colaboración, pero es deber del médico de atención primaria guiarlo a lo largo de la enfermedad. En la consecución de tal propósito, será necesario que el médico esté familiarizado con las técnicas, habilidades y objetivos de los especialistas y colegas en campos afines a la medicina.²³⁷.

²³⁴ BERROCAL LANAROT, Ana I, "La autonomía del individuo en el ámbito sanitario", Op. Cit., p. 235

²³⁵ Iniciativa, BOCG. Senado, III, A, 9 (a), 8 de febrero de 2001. Retirada, BOCG. Senado, III A 9 (b), 1 de marzo de 2001.

²³⁶ Vid. El hospital Vall d'Hebron de Barcelona realiza el tercer trasplante de cara en España, (en línea), El país, 29/03/2010, http://www.elpais.com/articulo/sociedad/hospital/Vall/d/Hebron/Barcelona/realiza/tercer/trasplante/cara/Espana/elpepusoc/20100329elpepusoc_10/Tes

²³⁷ VALENCIA MORENO, Alexander, Responsabilidad jurídica del médico y el seguro de responsabilidad médica, Instituto de Estudios Políticos e Internacionales Panamá, 1999, pág. 17

A su vez, esta LGS 14/1986 señala que la historia clínica estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y el tratamiento del enfermo, así como a efectos de inspección médica o para fines científicos, debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica. Ya desde este artículo vemos como se promueve el derecho de la intimidad y la protección de los datos del paciente, cuando señala la ley, quiénes son las personas que están autorizadas a acceder a este documento y las obligaciones que tal autoridad conlleva.

En si, el art. 61 de esta ley señala que en cada área de salud debe procurarse la máxima integración de la información relativa a cada paciente, pero a su vez dejó sin regular aspectos tan importantes como la naturaleza de la historia clínica, las condiciones de su acceso, los supuestos dueños del documento y lo concerniente a su depósito y término para su custodia. Las comunidades autónomas, en virtud del art. 148.21 de la CE, hicieron lo propio y tuvieron mayor desarrollo en este aspecto, lo que representó un gran apoyo, ya que por mucho tiempo llenó el vacío legal existente, previo a la aprobación de la LOAP 41/2002.

2.2. Antecedentes jurídicos de la historia clínica.

Tomamos como ejemplo de estas regulaciones anteriores, a las Comunidades Autónomas de País Vasco, Cataluña, Valencia, Galicia, Extremadura y Madrid.

País Vasco: Decreto 272/1986 de 25 de Noviembre por el que se regula el uso de la Historia clínica de los Centros Hospitalarios de la Comunidad Autónoma del País Vasco, establece:

Artículo 7.1: La información contenida en la Historia clínica tiene carácter de confidencial.

Artículo 8: 1. Los Centros Hospitalarios de la Comunidad Autónoma del País Vasco garantizaran la confidencialidad de toda la información contenida en las historias clínicas que se encuentren en su poder.

2. Asimismo, toda persona o institución que, de conformidad con el artículo anterior, tenga acceso a la información contenida en las historias clínicas deberá garantizar su confidencialidad.

Por otro lado, en el preámbulo define a la historia clínica como “el documento que contiene toda la información de utilidad clínica relativa al estado de salud o enfermedad de la población asistida en el Hospital, siendo un medio de comunicación muy valioso para transmitir esta información entre los distintos miembros que intervienen en el Plan de Asistencia al enfermo”.

Cataluña: Ley 21/2000, de 29 de diciembre, sobre los derechos de información concernientes a la salud y la autonomía del paciente, y la documentación clínica

Artículo 5.1: Toda persona tiene derecho a que se respete la confidencialidad de los datos referentes a su salud. Igualmente, tiene derecho a que nadie que no esté autorizado pueda acceder a ellos si no es al amparo de la legislación vigente.

Artículo 9.1: La historia clínica recoge el conjunto de documentos relativos al proceso asistencial de cada enfermo, identificando los médicos y demás profesionales asistenciales que han intervenido en el mismo. Debe procurarse la máxima integración posible de la documentación clínica de cada paciente. Esta integración debe hacerse, como mínimo, en el ámbito de cada centro, en el que debe existir una historia clínica única para cada paciente.

Galicia: Ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes.

Artículo 18: 1. Las historias clínicas son documentos confidenciales propiedad de la Administración Sanitaria o entidad titular del centro sanitario cuando el médico trabaje por cuenta y bajo la dependencia de una institución sanitaria. En caso contrario, la propiedad corresponde al médico que realiza la atención sanitaria.

2. La entidad o facultativo propietario es responsable de la custodia de las historias clínicas y habrá de adoptar todas las medidas precisas para garantizar la confidencialidad de los datos o de la información contenida en las mismas.

Asimismo, toda persona que en el ejercicio de sus funciones o competencias tenga conocimiento de los datos e informaciones contenidas en la historia clínica tendrá la obligación de reserva y sigilo respecto de los mismos.

Artículo 13: La historia clínica es el conjunto de documentos en los que se contienen los datos, valoraciones e informaciones de cualquier tipo sobre la situación y evolución clínica de los pacientes a lo largo de su proceso asistencial.

Extremadura: Ley 10/2001, de 28 de junio, de Salud de Extremadura.

Artículo 11. b y e: Al respeto de su personalidad, dignidad humana e intimidad, sin que puedan ser discriminados por ninguna causa. Este derecho incluirá el progresivo ofrecimiento de habitación individual en los centros hospitalarios de la Comunidad Autónoma de Extremadura.

A la confidencialidad de toda la información relacionada con su proceso y con su estancia en cualquier institución sanitaria de Extremadura.

Madrid: Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid.

Artículo 26.1: Son principios informadores de la organización y funcionamiento del Sistema Sanitario de la Comunidad de Madrid, la orientación al ciudadano como persona, su autonomía y la garantía de los derechos a la intimidad y a la protección de los datos de carácter personal

Artículo 27. 3 y 7: El ciudadano tiene derecho a mantener su privacidad y a que se garantice la confidencialidad de sus datos sanitarios, de acuerdo a lo establecido en la legislación vigente.

El derecho a la información sobre la propia salud incluye el acceso a la información escrita en la historia clínica, resultados de pruebas complementarias, informes de alta, certificados médicos, y cualquier otro documento clínico que contenga datos sanitarios propios. El grado de confidencialidad de los mismos debe ser decidido por el paciente.

Por último, hay que señalar que también existen otras comunidades autónomas con leyes muy parecidas como: Aragón (Ley 6/2002, de 15 de abril, de Salud de Aragón); La Rioja (Ley 2/2002, de 17 de abril, de Salud); Ley Foral 11/2002 de la Comunidad Autónoma de Navarra, sobre los derechos del paciente a las voluntades anticipadas, a la información y a la documentación clínica; Cantabria (Ley 7/2002, de 10 de diciembre, de Ordenación sanitaria de Cantabria); e Illes Balears (Ley 5/2003, de 4 de abril, de salud de les Illes Balear), pero

adentrarnos a detallar cada una de ellas, y la importante producción reglamentaria en cada caso, excede los límites impuestos en el presente trabajo.

No obstante, cada de una de estas regulaciones se hace con base a la facultad legal que posee cada comunidad autónoma, mediante la cual desarrolla aspectos particulares de cada región y atendiendo criterios de la población, siempre con la coherencia que la norma estatal exige para estos casos.

2.3. Aprobación de la Ley Orgánica de Autonomía del Paciente (LOAP) 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.

Aunque, como hemos dicho, las leyes autonómicas dieron la solución a muchos aspectos controvertidos que surgieron del art. 61 de la LGS 14/1986, sólo ostentaban el rango autonómico, y dejaban clara la necesidad de que se aprobara una nueva ley de carácter estatal, que brindara una definición más amplia en torno a los derechos del paciente y de su historia clínica. Además, en algunos casos, como el de Galicia, según crítica de SEOANE RODRÍGUEZ, la definición del concepto de historia clínica es de tipo descriptiva y no incluye referencia alguna a su finalidad. No es una definición exhaustiva o in extenso, aunque lo descrito en este precepto puede y ha de completarse con los artículos siguientes del propio Título III, en los que se examinan otros aspectos susceptibles de precisar el significado de la historia clínica.²³⁸

Es así que se aprobó la LOAP 41/2002²³⁹ fue para muchos, la oportunidad de volcar la gran experiencia y desarrollo normativo logrado por las comunidades autónomas en

²³⁸ SEOANE RODRÍGUEZ, José A., “¿A quién pertenece la historia clínica?”, en Revista de Derecho y Salud, Volumen 10, Número 2, Julio – Diciembre 2002, p.246

²³⁹ Publicada en el Boletín Oficial del Estado (BOE), número 274, de 15 de noviembre de 2002

una ley general y solucionar aspectos tan importantes como los ya mencionados. Sin embargo, aunque su valor es indiscutible, esta ley presenta entre otros casos, dos artículos en los cuales se define la historia clínica, y abre el debate nuevamente, ya que por una parte define su concepto en el art. 3 y después en el art. 14.1, nuevamente define el significado de historia clínica, aunque con otras variantes.

Art. 3. Las definiciones legales

...

Historia clínica: 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. 14. Definición y archivo de la historia clínica.

1. La historia clínica comprende 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. (la cursiva es nuestra)

Esta doble acepción ha sido criticada por algunos autores, debido a que las definiciones son diferentes, la primera más amplia y general que la segunda. Resulta un tanto contradictorio y pone de relieve una evidente falta sistemática del legislador, que en el art. 14 bajo la rúbrica general de “Definición y archivo de la historia clínica”, incorpore una definición diferente de la anterior, de carácter más descriptivo.²⁴⁰

De igual forma, tal como señala DE MIGUEL SÁNCHEZ, el capítulo III, centrado en el derecho a la intimidad del paciente, es realmente exiguo y constituye, a su modo de

²⁴⁰ DOMÍNGUEZ LUELMO, Andrés, Derecho sanitario y responsabilidad médica, Edit. Lex Nova, 2003, p.401

entender, la dejación más importante en que ha incurrido la ley al desaprovechar la oportunidad idónea para proceder a un reconocimiento tajante y explícito del derecho al secreto médico. Es evidente que de la conjugación de este capítulo con los artículos 2.7 y 16.6, en los que establece el deber de secreto para el personal que acceda a la documentación clínica, así como del contexto general de la ley, se deduce la existencia de este derecho²⁴¹. Es por esto que consideramos importante analizar la figura del secreto médico, no solo como un deber del profesional de la medicina, sino también como un derecho del paciente, aun cuando desde la Sentencia del Tribunal Supremo de 2 de julio de 1991, se establezca que el secreto médico es una modalidad del secreto profesional, un medio para proteger derechos fundamentales, pero no un derecho fundamental en sí mismo, sino un deber enderezado a evitar intromisiones ilegítimas en el ámbito de protección de la Ley 1/1982.

Más allá del debate sobre su correcta interpretación, esta LOAP 41/2002, sí logra ampliar otros aspectos fundamentales del dossier médico, como lo es definir cuáles son los documentos mínimos que deben conformarla, la obligación de establecer controles para su autenticidad, los usos que puede tener este documento, la conservación y derechos de acceso, así como el manejo de otros documentos importantes propios del ámbito clínico.

Siendo así, se comentarán algunas consecuencias de esta LOAP 41/2002, para el sistema sanitario y, en especial, su impacto en la historia clínica. Lo haremos con base en los aspectos más relevantes de este documento y las interpretaciones que se generan.

²⁴¹ DE MIGUEL SÁNCHEZ, Noelia, "Intimidad e historia clínica en la nueva Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica", en Civitas, Revista Española de Derecho Administrativo, número 117, año 2003, p 20 y 21.

2.4. Finalidad de la historia clínica.

La finalidad principal de la historia clínica está determinada en el art. 15.2 de la LOAP 41/2002, y señala que es facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. Dicho fin sirve de guía y facilita la asistencia sanitaria que realiza posteriormente el especialista de la salud. Asimismo, lo relevante no es el documento o conjunto de documento, sino lo que documenta, la perspectiva iusfundamental pone el énfasis en el contenido (decisiones y actos sanitarios que explican el devenir de la relación clínica), y no tanto en la forma o el soporte que documenta cada biografía sanitaria (el conjunto de documentos en los que consta: la historia clínica)²⁴². Desde aquí centramos también nuestra investigación, pues el papel archivado no es la materia que más nos interesa, más bien son los datos que contiene los que son especialmente merecedores de protección.

Cabe señalar que, además de su fin puramente médico, la historia clínica también puede ser utilizada para fines judiciales, la docencia, medir la calidad de atención y la investigación. Con ésta última podrían ampliarse nuevos descubrimientos sobre las patologías encontradas, terminando en publicaciones de corte científico). Para CASTELLANO ARROYO, la evolución moderna hacia la generalización de la medicina pública y la organización hospitalaria, así como los avances científicos y la proliferación de técnicas de exploración, han impuesto un ejercicio médico en equipo con la participación de numerosos profesionales sanitarios en el cuidado y atención a un mismo enfermo²⁴³. El autor destaca, además, que ya la historia clínica dejó de ser una narración biográfica muy personal, sobre las observaciones y los hallazgos clínicos y pasó a ser un documento imprescindible en la

²⁴² SEOANE RODRÍGUEZ, José A, Op. Cit. 249

²⁴³ CASTELLANO ARROYO, María, "Problemática de la historia clínica", en Información y documentación clínica, Madrid, Consejo General del Poder Judicial y Ministerio de Sanidad y Consumo, 1997, Vol. I, p.46

asistencia sanitaria cuyas repercusiones se extienden hoy a ámbitos como el legal, el administrativo, el científico etc.

La forma de elaborar y presentar esta historia clínica también está definida y, por primera vez, una norma estatal define cuáles son los elementos principales que debe contener dicha historia médica. En sí, el art. 15.2 final señala al menos dieciséis (16) tipos de documentos fundamentales en la historia clínica, excepcionando aquellos que no se apliquen por no tratarse de casos de hospitalización del paciente.

2.5. Características de la historia clínica.

Este documento posee características particulares, que se desprenden de las exigencias establecidas en la LGS 14/1986 y de la LOAP 41/2002. De ahí, que pasamos a analizar las siguientes características.

La historia clínica es un compendio de información confidencial que involucra elementos de la esfera privada del paciente, desde sus enfermedades anteriores, el perfil psicológico, los datos de domicilio, ingresos económicos y hasta su orientación sexual. De no guardar las debidas reservas, se podrían utilizar para actos de discriminación, chantajes y abusos a derechos.

Para acceder a esta información se requiere el consentimiento expreso del paciente, y todo dato que se genere producto de la gestión en salud es exclusivamente dirigido al paciente, y de ser consentido por éste a sus familiares.

Es un documento formal y exige a los médicos cierto tipo de comportamiento frente a la información que se pretende incluir, sobre todo porque de eso depende el trato que recibirá el paciente y otros usos que tendrá el documento. Es importante hacer

hincapié en lo siguiente: el médico puede señalar aspectos particulares sobre la atención o trato con el paciente en la historia clínica, pero no puede ser moralista en sus comentarios, ni apartarse del propósito fundamental que motivó su creación.

Los comentarios personales ajenos al propio tratamiento del paciente no deben ser incluidos, esta extrema previsión en cuanto a la solemnidad y claridad del documento, para algunos, ha cercenado parte de su riqueza haciéndolo muy frío y poco promotor de la investigación científica. Además de esto, la muy conocida “caligrafía” del médico también es objeto de cuidado, ya que debe procurar una escritura legible que pueda ser entendida no solo por quien hace la anotación, sino por todos los profesionales que se sirvan de ella. Con la utilización de historias clínicas informatizadas o electrónicas este aspecto se está superando, pero aun existen hospitales que dependen de una historia clínica en formato papel.

Es un documento con información precisa sin caer en el error de utilizar términos ambiguos o que conduzcan a errores de interpretación. Sin embargo, este documento no es necesariamente una biografía agotadora de un acontecimiento asistencial, en si, una de las características más importante es la coherencia de la información reflejada en la historia clínica, aquella documentación presentada en orden cronológico²⁴⁴, que demuestre cómo evolucionó la estancia del enfermo en el centro asistencial y cómo fue el trato dispensado por el médico, amén de todos los datos adjuntos, pruebas de laboratorios practicadas, informes de anestesia, constancia de consentimiento informado, informes de alta, etc.

Es muy importante “el momento” para la elaboración de la historia clínica, los hechos deben anotarse con la mayor prontitud posible. Esperar, en ocasiones, da pie al olvido de detalles que bien pudieran ser importantes tanto para el paciente, como para la

²⁴⁴AYERRA LAZCANO, José M., “Regulación general de la historia clínica”, en Revista Derecho y Salud, Volumen 11, número 1, Enero Junio 2003, p.28

propia seguridad jurídica del médico. Es por eso que la LOAP 41/2002 obliga que, además, de los datos, se incluya fecha y hora. Del mismo modo, esta información debe ubicarse en el respectivo Hospital o Centro de Atención. La LOAP 41/2002, en su art. 14.2, exige que cada centro archive las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

Esta disposición acaba con el debate sobre la posesión de la historia clínica, pues reitera que es responsabilidad del centro sanitario, por lo menos en la custodia de dicho documento. Asimismo, formaliza la posibilidad que tienen los hospitales y centros de atención primaria para utilizar las nuevas tecnologías, en caso de optar por la informática para la conservación de las historias clínicas.

La norma dispone, además, que las historias clínicas se conserven en el sitio en el que recibe atención el paciente, sirviendo de apoyo inmediato para el médico que atiende al enfermo por última ocasión. En este tema se ha debatido también sobre quién debe custodiar los archivos y si es posible “externalizar” esta función en terceros (compañías especializadas), por motivos de espacio o por actualización de los expedientes. En este sentido, la LOPD 15/1999 establece en su art. 12 que “no se considerará 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”. Asimismo, la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas, una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual

que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

Este historial es único, y debe tener integración y unidad de la información. Aunque existan varios servicios que presta un centro de asistencia u hospital, deberá existir un solo expediente por cada paciente, tratando de que las diversas atenciones recibidas sean debidamente organizadas, para que los especialistas puedan comprobar el nivel de evolución que ha tenido el enfermo en cada aspecto de atención. Dicho esto, es preciso inmediatamente señalar que esa integración de la historia clínica, tendente a evitar la dispersión de la información sanitaria sobre cada paciente, tiene como beneficiario al propio paciente. El inciso inicial del art. 16 de la LOAP 41/2002 es paladinamente claro a este respecto: "la historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente." Ciertamente, permiten prestar una asistencia sanitaria mejor; pero esta mejora no se justifica por el ahorro de esfuerzo para terceros (el personal sanitario, la Administración, los empresarios, etc.), sino por el bienestar del paciente. Este punto es de crucial importancia, porque la información sobre la salud de las personas forma parte del objeto protegido por el derecho fundamental a la intimidad, tal como ha aclarado, entre otras, la Sentencia del Tribunal Constitucional 196/2004.²⁴⁵

Por otro lado, la historia clínica de un paciente reunirá la información concerniente a los aspectos científicos, técnicos y administrativos de la atención en salud en las fases de fomento, promoción, prevención específica, diagnóstico, tratamiento, recuperación y rehabilitación de la salud, considerando al paciente integralmente y en sus relaciones con los ámbitos biológicos, psicológico y social, e interrelaciones con sus dimensiones personal, familiar y comunitaria. Estos datos no clínicos pueden ser determinantes para entender cómo llegó el paciente, cuáles han sido las condiciones que se

²⁴⁵ STS, de 20 de octubre de 2009, FJ: 5 (RJ 2009\7551)

involucraron para la existencia de la enfermedad, siendo precisamente esta integralidad la que realmente puede explicar de mejor forma la situación que vive la persona.

Asimismo, este es un documento de comunicación entre médicos a lo largo del tiempo, ya que varios especialistas pueden atender al mismo paciente, en un mismo centro hospitalario. Por tal motivo, la historia clínica servirá de medio idóneo de comunicación entre los médicos que intervengan en el trato del paciente. Con esta información se puede hacer una cronología del enfermo y verificar si es prudente mantener el tratamiento o cambiarlo de acuerdo a la evolución del paciente.

2.6. La titularidad en la historia clínica.

El debate sobre la propiedad de la historia clínica no es nuevo es más, fue ampliamente analizado en España desde años atrás, pero con mayor desarrollo en las legislaciones autonómicas. Señalamos esto porque la LOAP 41/2002 sólo se refiere a la custodia de este documento, pero no aclara en definitiva quien tiene la “propiedad” del mismo. De esto, también llama la atención que la ley no hable de propiedad de la historia clínica. Tal vez sea como consecuencia de los múltiples derechos que surgen de esta, por lo que el legislador no ha querido plantear el problema en dichos términos, sino teniendo en cuenta que en este conjunto de documentos que conforman la historia clínica convergen intereses jurídicamente relevantes: los del paciente, los de los profesionales sanitarios, los del centro, en incluso un interés público, como es el caso de la investigaciones de enfermedades.

Y ya que usamos el vocablo propiedad, por así hacerlo muchas leyes autonómicas en su redacción, coincidimos en la opinión que este término no es el más adecuado, con respeto al verdadero vínculo que existe entre este documento y sus usuarios. La verdad es que nos parece más ajustado a la realidad utilizar el concepto de titularidad, que se refiere a

los derechos que se tienen sobre la historia clínica, en reemplazo de “propiedad”, que se refiere a un vínculo muy patrimonial que no se compadece con la realidad que viven los enfermos, los médicos y los hospitales. La titularidad de derechos, a nuestro criterio, se ajusta a las verdaderas características de la historia clínica, pues no se puede desconocer que en la práctica se sirven de ella distintos usuarios, cada uno con un propósito particular o diferente. Siendo así, al constituirse como derechos se generan también obligaciones, las cuales pueden ser exigidas por todos los que mantengan un vínculo con la documentación del paciente.

En algunas leyes autonómicas, como el caso de la Ley 3/2001 de 28 de mayo, Reguladora del Consentimiento Informado y de las Historias Clínicas del paciente (Galicia), sí se desarrolla con más claridad este tema. En su art. 18 dice que “las historias clínicas son documentos confidenciales propiedad de la Administración Sanitaria o entidad titular del centro sanitario cuando el médico trabaje por cuenta y bajo la dependencia de una institución sanitaria”. En caso contrario, la propiedad corresponde al médico que realiza la atención sanitaria. La entidad o facultativo propietario es responsable de la custodia de las historias clínicas y habrá de adoptar todas las medidas precisas para garantizar la confidencialidad de los datos o de la información contenida en las mismas. Asimismo, toda persona que en el ejercicio de sus funciones o competencias que tenga conocimiento de los datos e informaciones contenidas en la historia clínica tendrá la obligación de reserva y sigilo respecto de los mismos.

En igual medida, la Ley 1/2003, de 28 de enero, de la Generalitat, de Derechos e Información al Paciente de la Comunidad Valenciana establece, en su art. 23, que las historias clínicas son documentos confidenciales propiedad de la Administración Sanitaria o entidad titular del centro sanitario cuando el médico trabaje por cuenta ajena y bajo la dependencia de una institución sanitaria. En caso contrario, la propiedad corresponde al médico que realiza la atención sanitaria.

Sorprende que siendo un tema tan debatido, el legislador no lo haya tomado en cuenta para resolver lo pertinente a este tema en la propia LOAP 41/2002, ya que evitó hablar de propietario de la historia clínica, y solamente se refirió a la custodia y archivo de los documentos. Siendo así, aun persisten en reclamar primacía las tres partes fundamentales: por un lado, el paciente, quien se considera base principal del documento: el médico, por ser quien analiza y crea el historial, y la institución por ser quien archiva y custodia la historia clínica.

2.6.1. Del paciente.

Algunos autores como GARCÍA HERNÁNDEZ Y MARZO MARTÍNEZ, sostienen que como el paciente es la fuente de la historia clínica, le pertenece la propiedad sobre la misma, pues aporta su propia información y persona para su elaboración²⁴⁶. En definitiva, los que sostienen esta posición afirman que el paciente arrienda los servicios del médico, y éste tiene, entre sus obligaciones, la realización del historial médico. Nos parece que esta posición sólo toma en cuenta la perspectiva del paciente que, aunque se le reconoce una cotitularidad en los derechos sobre la historia clínica, difícilmente puede excluir con su derecho, las facultades que otros usuarios también tienen con el documento.

La atribución del derecho de propiedad a favor del paciente tendría su fundamento principal, según sus defensores, en que el origen de la historia clínica siempre es el paciente y toda la información en ella contenida está referida a su persona, sin perjuicio de su utilización por el Centro Sanitario, y por el médico que la crean y actualizan. Sin embargo, el paciente no tiene potestad para introducir ni quitar dato de la historia clínica, ni para

²⁴⁶ GARCÍA HERNÁNDEZ, Tomás y MARZO MARTÍNEZ, B, La propiedad de la historia clínica, Edit. La Ley, 1996, p. 1629 y ss.

custodiarla²⁴⁷. En este aspecto se podría aplicar, en primer término, la autodeterminación informativa, cuyo fundamento es el art.18.4 de la CE. Pero, éste sólo abarcaría la información que se incluirá en el historial, con base a la confidencialidad de los datos de salud. Siendo así, el paciente es titular de la intimidad en los datos que se incluyen en la historia clínica, con facultades para corregirlos o anularlos cuando exista algún error, debidamente comprobado.

En defensa del derecho exclusivo del paciente se toma como fundamento legal, lo establecido por la literalidad del punto 5.6º del Anexo I del Real Decreto 63/1995, de 20 de enero, de Ordenación de Prestaciones Sanitarias del Sistema Nacional de Salud, en el que se alude al derecho del paciente a la comunicación o entrega de “un ejemplar de su historia clínica.” (el subrayado es nuestro).

Esta posición del derecho de propiedad del paciente no es del todo satisfactoria pues, aunque el paciente sea la base para elaborar la historia clínica, no significa que el expediente que se conforme le pertenezca totalmente. Es así, ya que al compararlo con la práctica judicial en la que los abogados, aunque promueven la causa ante el tribunal, en nombre del cliente, no son dueños del expediente, ni siquiera al terminar el proceso. Lo que si puede hacer es obtener copias compulsadas del mismo y el tribunal se reserva el derecho de archivo y custodia. Además, hoy en día, la historia clínica se elabora cada vez con más frecuencia por equipos de profesionales multidisciplinares. En tal sentido, MÉJICA GARCÍA señala que existe la necesidad de contemplar los derechos y obligaciones de todos los intervinientes, esto es, los facultativos que la elaboran, los pacientes para cuya asistencia se deja constancia de datos personales y científicos y los centros sanitarios que las custodian. Y

²⁴⁷ SAMPRÓN LÓPEZ, David, Los derechos del paciente a través de la información y la historia clínica, Edit. Edisofer S.L., p. 59

todo ello en una sociedad que presta especial atención a la defensa de la intimidad de las personas, como el libre ejercicio del derecho a la difusión de la información²⁴⁸

2.6.2. Del médico.

Para MARTINEZ CALCERRADA, el “dominio jurídico del médico (poder de uso, disfrute y disposición), sobre la historia clínica deriva de que ésta no es una mera transcripción de datos o noticias suministrados por el paciente, sino el resultado de un proceso de recogida, ordenación y elaboración”. La propiedad intelectual del médico sobre la historia clínica se basa en el derecho de autor y para ello no basta la mera recopilación de datos, sino que el médico, mediante una labor de análisis y síntesis, transforma la información recibida, con resultado de una creación científica, expresada en términos de valor terapéutico, diagnóstico, pronóstico y tratamiento.²⁴⁹ Esta afirmación del autor se comparte parcialmente. Efectivamente, el profesional es titular del uso, disfrute y disposición de este documento, pero todo derecho tiene sus límites y, en el caso del médico, no es un derecho absoluto, ya que está condicionado a la intimidad y a la protección de los datos del paciente. Del mismo modo, el médico tiene garantizada su intimidad en el historial clínico, ya que en este documento también queda reflejada su participación y con cada anotación que realiza, se puede generar su perfil profesional, lo que lo haría identificable ante el resto de los profesionales que le rodean y los usuarios en general. Estos datos serán considerados como datos protegidos o subjetivos.

Ahora bien, el derecho del médico se ve ampliamente reforzado en aquellos casos en los que el profesional realiza la práctica privada de su profesión, en la cual, dado

²⁴⁸ MÉJICA GARCÍA, Juan M., La historia clínica: Estatuto básico y propuesta de regulación, Edit. Edisofer SI, 2002, p. 16

²⁴⁹ MARTINEZ CALCERRADA, Ricardo, Derecho médico – tratado de derecho sanitario, Tomo 1, Asociación Española de Derecho Sanitario, 2001, p. 773

que su trabajo no obedece a la contratación con un empleador, el resultado de su investigación, pertenece en cierto modo, al facultativo. Se hace esta aclaración pues es aceptado que, cuando el médico realice su labor conforme a un contrato de trabajo con un empleador, dicha producción se entenderá propiedad del centro sanitario que le ha contratado para prestar sus servicios como médico, siéndole imposible esgrimir el derecho de autor sobre la información que se genere producto de la asistencia médica, con excepción a aquella labor realizada por el médico en cuanto a tratamiento de psiquiatría, siempre y cuando se elaboren las correspondientes reservas, plenamente aceptadas entre el médico y el centro sanitario.

Sobre el particular, los que defienden el “derecho de autor” del médico, como parte de la “propiedad intelectual”, encuentran difícil el encaje de dicho concepto en la Ley 22/1987, que regula la propiedad intelectual en España. Dicha norma, en su artículo 10, indica “que son objeto de propiedad intelectual todas las creaciones originarias literarias, artísticas o científicas expresadas por cualquier modo o soporte, tangible e intangible, actualmente conocido o que se invente en un futuro”. Siendo así, queda la duda en cuanto a si la historia clínica puede ser considerada una creación literaria, artística y científica, parece claro que no es una obra literaria ni artística y tampoco una obra científica, per se. Adicionalmente, aclara la propia Ley 22/1987, este tema, cuando señala en su art. 51, que la persona empleada se obliga a la transmisión al empresario de los derechos de explotación de la obra, creada en virtud de la relación laboral estará regida por lo pactado, debiendo realizarse éste por escrito. A falta de pacto escrito se presumirá que los derechos de explotación han sido cedidos en exclusiva y con alcance necesario para el ejercicio de la actividad en virtud de dicha realización laboral.

En este sentido, para esta parte, es importante el “elemento intelectual” del médico, ya que dicho profesional no es solo un colector de datos proporcionados por el paciente, además de esta labor, analiza cada detalle y le imprime el conocimiento propio de

su especialidad, llegando a la formulación del diagnóstico, pronóstico y tratamiento para el enfermo. Lo anterior es correcto y también es admirable el esfuerzo que representa el tratamiento de la enfermedad, pero, la tesis cotitular del derecho, no es incompatible con el derecho del médico a usar los datos y del paciente de acceder a la historia clínica cuando lo considere necesario, salvo las limitaciones de rigor, como son, la tenencia permanente del documento y la facultad de adicionar o retirar, parte de su contenido, sin previo análisis.

2.6.3. De la Administración.

La LOAP 41/2002 dice, en su art. 17.1, que “los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial”. Esto en algunas ocasiones ha permitido que se confunda lo dispuesto por el legislador, con un supuesto derecho de “propiedad”, a favor de los centros sanitarios. De no cumplir con este deber de custodia, puede resultar sancionado, como el caso acogido mediante resolución R/02182/2010, proferida por la Agencia de Protección de Datos, en la que se obliga al centro hospitalario a “adoptar las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 9.1 de la LOPD”²⁵⁰. Esta obligación, hace especial hincapié en el artículo 106 en relación con los criterios de archivo a implantar que posibiliten, entre otras cosas, el ejercicio del derecho de acceso.

En relación con esta cuestión, es importante aclarar que no se puede confundir un deber reforzado por la ley, con un derecho, pues el deber de conservación o custodia de la historia clínica no equivale a la propiedad, ni tampoco a la titularidad de los derechos. La obligación de custodia guarda lógica con la titularidad de derechos que asiste, tanto al

²⁵⁰ AGENCIA DE PROTECCIÓN DE DATOS, Resolución R/02182/2010, de 30 de diciembre de 2010, Rv: 2.

paciente como el médico, pues para cumplir con estos principios, la institución o centro sanitario será el garante de la correcta conservación del dossier y tendrá a su cargo la obligación de establecer procedimientos que igualmente protejan los datos de ambas partes. En si, la titularidad de pacientes y médicos no se transfiere al centro sanitario, por no corresponder esto con la lógica jurídica; más bien surge un deber designado por la ley, para la protección adecuada de la información que corresponde a la salud de los ciudadanos. Esto hace alusión a mantener su integridad, a fin de que no se disperse su contenido o se conserve en forma desordenada.

Lo que más preocupa es que esta obligación pueda mal interpretarse como un derecho para negar el acceso a la historia clínica, sin fundamento legal, condicionando a sus titulares a la concesión o privilegio que decida otorgar, unilateralmente, el centro sanitario. No sorprende que existan hospitales que, sin tener bases jurídicas, hacen difícil el acceso de pacientes y médicos a las historias clínicas, estableciendo procedimientos excesivamente burocráticos o tasas que desbordan la intención de la ley.

2.6.4. Posición ecléctica e integradora.

Como es regular en estos casos, existe una posición conciliadora, que se acerca mucho a la conciliación para la partes, ya que trata de incorporar las diversas posiciones y logra la creación de una postura común. Esta tesis sostiene que no son excluyentes los derechos planteados por cada parte (paciente y médico), y el deber del centro sanitario. Por el contrario, cada uno tiene su fundamento desde diferentes aspectos. Efectivamente, el centro sanitario es garante de la historia clínica, pues se encarga de su archivo y custodia, al paciente se le reserva ser el titular de la intimidad de sus datos y la autodeterminación informativa y al médico la intimidad de su gestión profesional y la facilidad de usar y tener a disposición dicho documento.

La historia clínica, dados sus múltiples usos, tiene una “propiedad tripartita”, del médico, del paciente, del centro sanitario y, en consecuencia, todos con derecho de acceso. Del médico, porque la confecciona; del paciente, porque allí debe constar su proceso existencial y de la institución porque debe ser garante de su conservación. De todo esto se deduce que, más que el protagonismo por reclamar “la propiedad del documento”, se debe velar por su acceso, la garantía confianza y seguridad que debe otorgar a la práctica médica; y la protección de los pacientes y demás usuarios.

2.7. Acceso a la historia clínica.

Los problemas relativos al acceso a la información de la historia clínica suelen estar precedidos de discusiones doctrinales relativas a la naturaleza y propiedad de dicha historia. Y así, unos sostienen la teoría de la propiedad del paciente, otros la teoría de la propiedad del médico o del centro sanitario, y, en fin, no faltan teorías integradoras o eclécticas, las cuales ya hemos mencionado.

El acceso a la historia clínica es razonadamente limitado y aunque es un documento manejado por varias personas con diversos motivos, esto no significa que su uso sea libre sin mantener las reservas de ley, salvo aquellos casos en los que se autorice y resguarde la confidencialidad de la información. Ya hemos mencionado que la confidencialidad de la información atribuida a la historia clínica, en atención a la intimidad del paciente, impide que otros puedan ingresar a esta libremente, sin el cumplimiento de requisitos establecidos por la ley. En cuanto al concepto acceso, nos referimos también a la posibilidad visualizar el documento o de obtener copias del mismo. (ver capítulo 5.2.1.)

La LOAP 41/2002 establece, en su art. 7.1, que el paciente tiene, ante todo derecho a su intimidad, por lo que sus datos se consideran sensibles y por ende confidenciales. El art. 8.4 establece que, además, el paciente debe ser advertido y a la vez

consentir en caso de que se pretenda utilizar su historia clínica como base para investigaciones, docencia y control de calidad. Obviamente, esto no puede conllevar ningún tipo de riesgo adicional a la salud de la persona. Del mismo modo, la LOPD 15/1999 establece que el acceso a la historia clínica con otros fines asistenciales, obliga a preservar los rasgos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de modo que, como regla general, quede asegurado el anonimato, salvo que el propio paciente hubiese dado su consentimiento para no separarlos.

Sobre esta misma materia, se aprobó el reglamento de la LOPD 15/1999, mediante Real Decreto 1720/2007, que también ampara a las historias clínicas, el cual intenta conciliar las muchas perspectivas y los distintos intereses sociales que afectan a la aplicación de la normativa de protección de datos²⁵¹.

Ahora bien, en este documento existe una gran complejidad, pues no solo acceden a éste el médico. Por el contrario, el personal sanitario se sirve de su información y adjunta documentación pertinente a su respectiva especialidad. La LOAP 41/2002 indica que todas las personas que acceden al historial clínico de un paciente están obligadas a mantener en estricta reserva los datos allí contemplados y la confidencialidad propia del expediente. Esta obligación, también recae sobre los hospitales o servicios de salud, los que tendrán que establecer medidas que aseguren la protección de los derechos de los pacientes. Sin embargo, no basta con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva²⁵².

²⁵¹ RALLO LOMBARTE, Artemi, “Uno de los principales retos en la actualidad es dar respuesta preventiva y no sólo represiva a la protección de datos personales”, en Revista Lex Nova, Abril – Junio, Número 52, 2008, p.10

²⁵² SAN, de 12 de noviembre de 2008, FJ: 2 (JUR 2008\380816)

Como es un documento en constante construcción, hay que reconocer que está sometido a muchas consultas. Esto conlleva que existan flujos y manejos de entrada y salida de la historia clínica del archivo y las personas responsables de los mismos deben velar por su custodia y conservación, debido al carácter confidencial y de reserva de la historia clínica. En adelante, revisaremos quiénes pueden acceder a este documento y cuáles son los límites a su derecho.

2.7.1. El acceso a la historia clínica por el paciente.

La LOAP 41/2002, en su art. 18, dice que el paciente tiene el derecho de acceso, con las reservas establecidas en la propia ley, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Las reservas a que se refiere implica que el derecho al acceso no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en la historia clínica 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 cumplimiento de este derecho no ha sido fácil. El hecho de que la historia clínica incorpore datos personales y que una pluralidad de sujetos pueda tener acceso a éstos, lo hace muy complicado, sobre todo por las “reservas” contempladas en la ley. Este derecho se dificulta aún más cuando el expediente solicitado contiene datos aportados por terceros o del propio médico que en ninguna medida hubiesen incluido si dicha información es de libre acceso para el paciente. No obstante, si se ejerce el derecho de acceso ante el responsable de la custodia de la historia clínica y éste trata otros datos personales del

afectado que no figuran en ella, deberá permitir su ejercicio también respecto de dicha información²⁵³.

Esta dualidad, entre el derecho del paciente al acceso de su historial clínico y el derecho de otros a mantener en reserva su información, ha provocado que todavía no se pueda definir, con claridad meridiana, qué datos son de interés para el paciente y cuáles no. Y es que el médico, dentro del análisis socio familiar del paciente, puede hacer sus propias anotaciones personales o preguntar a familiares, padres, cónyuges u otros, algunas “costumbres” de sus pacientes, que le ayuden a configurar y detectar la patología que aqueja al enfermo. Esta información podría ser confidencial y no accesible al enfermo.

Es más, los propios médicos en ocasiones, en virtud de la reserva del expediente, incluyen apreciaciones privadas, pero vinculadas con el tratamiento. Por ejemplo, paciente con múltiples lesiones corporales “presenta rasgos de posibles trastornos psicológicos, requiere ser tratado por especialista en la materia”. Si esta anotación es de libre acceso para el paciente, posiblemente no la asimilaría desde un enfoque clínico asistencial, sino como un ataque personal, pudiendo inclusive presentar alguna reclamación.

Lo interesante es que esta información, en ocasiones, enriquece el propio historial clínico y ayuda a entender cómo inciden otros factores en la salud del paciente. En consecuencia, el riesgo a posibles reclamaciones futuras ha mermado las anotaciones al margen de lo estrictamente exigible, lo que ha reducido la trascendencia de la historia clínica para los propósitos de docencia o investigación, e incluso, la información con fines terapéuticos adicionales.

²⁵³ RUBI NAVARRETE, Jesús, “Experiencia y criterios de la Agencia de Protección de Datos (AEPD), sobre los datos personales de la salud”, en RIPOLL CARULLA, Santiago (ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Agencia Catalana de Protección de Datos, Ediciones Jurídicas y Sociales S.A., 2006, p.282

He aquí parte de la controversia: ¿hasta dónde se puede decir que un dato que aparece en la historia clínica del paciente debe tener el carácter “reservado”? y, por ende, no puede ser entregado al paciente. Desde una perspectiva simple, todos los datos que impliquen intervención de terceros o comentarios del médico no pueden ser incluidos. Pero, ¿qué sucede con el paciente que necesita documentos concretos dentro del expediente, pues tiene que probar que la atención que realizó el médico no fue correcta?, ¿cómo obtiene la prueba completa de esa mala atención?, si su expediente, de acuerdo con la ley, “pasa por un filtro” antes de serle entregado.

Cabe señalar que una de las funciones de la historia clínica es servir de prueba casi vital ante las reclamaciones judiciales del paciente, y es él quien debe demostrar la culpa del médico, conclusión que, según GARCÍA HERNÁNDEZ, ciertamente debe ser revisada por exigir al paciente que vea donde no puede ver, que conozca donde no le es posible llegar, que aporte la prueba que no dispone, que posea conocimientos que sólo el médico conoce, etc. En definitiva, se pide al paciente algo imposible de conseguir. Se le pide una prueba diabólica, para demostrar lo que de forma muy sencilla podría demostrar el verdadero actor de la escena: el médico²⁵⁴. No obstante, se va abriendo camino la tesis de no hacer recaer exclusivamente sobre la parte perjudicada la carga absoluta de la prueba, para no producir indefensión por la dificultad de encontrar profesionales médicos que emitan un informe que pueda ser negativo para otro profesional de su misma clase²⁵⁵.

De lo anterior, es importante señalar que, para que pueda surgir la responsabilidad del personal sanitario o del centro de que aquél depende, como consecuencia del tratamiento aplicable a un enfermo, se requiere ineludiblemente que haya intervenido culpa

²⁵⁴ GARCÍA HERNÁNDEZ, Tomás, Elementos de derecho sanitario en la responsabilidad civil y penal de los médicos por mala praxis, Edit. Edisofer, S.L., p. 85

²⁵⁵ SAP, 268/2003 de Las Palmas, de 22 de abril de 2003, FJ: 1 (AC 2004\300)

o negligencia por parte del facultativo que realizó el acto médico o clínico enjuiciado, ya que, en la valoración de la conducta profesional de médicos y sanitarios en general queda descartada toda responsabilidad más o menos objetiva, sin que opere la inversión de la carga de la prueba admitida para los daños de otro origen, siendo imprescindible que a la relación causal, material o física, haya de sumarse el reproche culpabilístico, que puede manifestarse a través de una negligencia omisiva en la aplicación de un medio curativo o, más generalmente, en la existencia de una acción culposa o negligente en tal aplicación²⁵⁶. La razón de este rechazo hay que situarla en el hecho de que, a diferencia de otras actividades que se despliegan en beneficio propio de su autor (por lo que sí crea los riesgos debe estar a sus consecuencias dañosas y debe, entonces, probar que no incurrió en culpa), la actividad médica generadora del riesgo se pone en práctica, precisamente, en beneficio, no del que la realiza, sino del destinatario, del paciente y con su consentimiento, en la medida que busca remediarle un mal o padecimiento²⁵⁷.

Sin embargo, la jurisprudencia del Tribunal Supremo ha ido evolucionando en el sentido de aplicar también a los supuestos de responsabilidad médica el criterio de la facilidad probatoria, sobre todo, en lo que atañe a los centros sanitarios. Por ejemplo, tal como señala en sentencia, “siguiendo a la doctrina angloamericana y alemana según la cual ante un resultado desproporcionado, la cosa habla por sí misma “res ipsa loquitur” y hay clara apariencia de prueba “Anscheinsbeweis” de la culpa, culpa virtual “faute virtuelle” que si no consta la negligencia de médicos concretos, sí aparece, como dice la Sentencia de 2 de diciembre de 1996, una presunción desfavorable que pueda generar un mal resultado, cuando éste, por su desproporción con lo que es usual comparativamente, según las reglas de la experiencia y el sentido común, revele inductivamente la penuria negligente de los

²⁵⁶ SAP, 83-2003 de Madrid, de 29 de enero de 2003, FJ: 4 (AC 2003\1159)

²⁵⁷ SAP, 478-2002 de Pontevedra, de 31 de diciembre de 2002, FJ: 3 (AC 2002\2302)

medios empleados, según el estado de la ciencia y las circunstancias de tiempo y lugar, o el descuido en su conveniente y temporánea utilización”²⁵⁸.

En este sentido, la prueba de la relación de causalidad (así como la de la culpa) incumbe al paciente, y no al médico. Cabe aclarar que, este criterio tiene algunas excepciones, entre las que figuran cuando se produce un daño anormal y desproporcionado²⁵⁹ entre la intervención médica y el daño. En cuanto a este último aspecto cabe citar, entre otras, las Sentencias del Tribunal Supremo de 31 de julio de 1996 (indicios muy cualificados por anormales), de 2 de diciembre de 1996 (la parte que se halle en mejor posición probatoria por su libertad de acceso a los medios de prueba), de 28 julio de 1997 (la mejor posición probatoria en el supuesto de que surjan complicaciones que no son consecuencia natural o previsible del propio curso de la enfermedad no puede excusar de contribuir activamente a probar que no hubo negligencia o imprevisión por su parte), de 19 febrero de 1998 (que alude a la obstrucción o falta de cooperación del médico cuando el daño al paciente es desproporcionado), de 29 julio de 1998 (cuando se debían haber ofrecido explicaciones convenientes de los hechos), de 28 de diciembre de 1998 y de 19 de abril de 1999 (la carga de la prueba recae sobre el profesional de la medicina por ser quien se halla en una posición más favorable para conseguir su prueba) y de 31 de julio de 2002.²⁶⁰

²⁵⁸ SAP de Barcelona, de 20 de septiembre de 2002, FJ: 4 (AC 2002\1729)

²⁵⁹ El daño desproporcionado es aquel no previsto ni explicable en la esfera de su actuación profesional y obliga al médico a acreditar las circunstancias en que se produjo por el principio de facilidad y proximidad probatoria. Se le exige una explicación coherente acerca del porqué de la importante disonancia existente entre el riesgo inicial que implica la actividad médica y la consecuencia producida, de modo que la ausencia u omisión de explicación puede determinar la imputación, creando o haciendo surgir una deducción de negligencia.

²⁶⁰ STS, 1288-2002 , de 23 de diciembre de 2002, FJ: 3 (RJ 2003\914)

2.7.2. El acceso a la historia clínica por el médico.

El médico, como ya mencionamos, es titular de uso, disfrute y disposición de la historia clínica de su paciente, por lo que no tiene mayor problema en acceder a este documento. Sin embargo, su acceso está condicionado al registro de las actuaciones que haga sobre este documento, ya que en adelante se le exigirá que pruebe que proporcionó información al paciente sobre todas aquellas circunstancias relacionadas con la intervención mientras éste se halle bajo su cuidado, pues se trata de hechos que fácilmente pueden ser probados por él y que integran, además, una de sus obligaciones fundamentales²⁶¹.

Por otro lado, el derecho de acceso expedito del médico a la historia clínica conlleva una obligación inmediata, que es tratar al paciente conforme a este documento y preparar en consecuencia su intervención bajo dicho términos. De no hacerlo, se ubica con toda claridad en el ámbito de la temeridad, es decir, en el marco de la imprudencia temeraria profesional, pues, cuando la culpa recae en un profesional que tiene saberes y posibilidades específicas de actuación, las reglas socialmente definidas alcanzan un mayor grado de exigencia, pues no son ya las comunes exigibles a cualquier persona, sino que incluyen las del conocimiento y aplicación de los saberes específicos para los que ha recibido una especial preparación técnica avalada por un título facultativo que certifican esos especiales y específicos conocimientos en el campo en el que desarrolla su actividad profesional, con lo que la inobservancia de esas reglas que deben presidir su actuación generan un plus de antijuridicidad y, por consiguiente, un mayor reproche penal en relación con los bienes jurídicos afectados por las actuaciones que requieren un especial cuidado en su ejercicio, de suerte que la imprudencia del profesional en el ejercicio de su campo propio se perfila como una mayor gravedad en función del mayor nivel de exigencia a que éstos están obligados precisamente por disponer de una cualificación técnica sobre la actividad que desarrollan.²⁶²

²⁶¹ STS, 743-2008, de 28 de noviembre de 2008, FJ: 3 (RJ 2008\4638)

²⁶² STS, 308-2001, de 26 de febrero de 2001, FJ: 2 (RJ 2001\1340)

En otro orden de ideas, ni siquiera los propios médicos pueden ir consultado cuanta historia clínica se les ocurra,²⁶³ ya que podrían ser objeto de procesos judiciales. Por esto, sólo pueden consultar las historias clínicas de los pacientes que tienen asignados, por temas estrictamente asistenciales y bajo los criterios que establece la LOPD 15/1999. Surge otra obligación para los médicos: abstenerse de consultar los datos más allá de los que tiene en su propia consulta. Pero, ¿cuánto de esto realmente se cumple? Las respuestas oscilan entre "escasísimamente", si se pregunta a los profesionales en las trincheras y "relativamente", en las posiciones más diplomáticas de las autoridades sanitarias y los organismos colegiales.²⁶⁴

2.7.3. El acceso a la historia clínica por los familiares y terceros.

La LOAP 41/2002 determina que los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. Siendo así, entendemos lo razonado por la Audiencia Provincial cuando señaló que no puede admitirse que, junto con la historia clínica, se acompañe un informe explicativo. Y ello por dos razones: la primera, que lo único a que da derecho la ley es al acceso a la historia clínica, la segunda, porque a través del informe explicativo se podría buscar un sucedáneo de prueba pericial y de reconocimiento de hechos

²⁶³ STS, 1328-2009, de 30 de diciembre de 2009, FJ: 10 (RJ 2010\437)

²⁶⁴ VALLÉS. PALMA, Matías, La sentencia que ha alarmado a la clase médica balear,(en línea), diariodemallorca.es,1/3/2009,http://www.diariodemallorca.es/secciones/noticia.jsp?pRef=2009030100_2_440525__MALLORCA-sentencia-alarmado-clase-medica-balear

desfavorables, y las medidas de exhibición no están previstas para esas otras rentabilidades adicionales²⁶⁵.

En otros casos, cuando se tenga un interés legítimo o una justa causa, podrá tenerse acceso mediante el respectivo proceso judicial. En definitiva, de acuerdo a la LOAP 41/2002, los derechos de acceso son solo para el paciente, los médicos encargados de su tratamiento y el centro hospitalario, y solo se tomará en cuenta a los familiares que el propio paciente haya autorizado. Sin embargo, para solicitar la historia clínica de un familiar fallecido, primero debe agotarse la vía directa ante el hospital²⁶⁶, por ser éste el custodio original de tal documento. Y, de no obtener resultado, por inconvenientes o por razones infundadas, se puede proceder mediante la vía judicial. De esta manera, el Tribunal sólo intervendrá como apoyo de quienes, siguiendo el procedimiento, no hayan obtenido respuesta por parte de los centros sanitarios.²⁶⁷

En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros. En estos casos se prevén situaciones en los que el interesado tenga dudas sobre si la convivencia con el paciente fallecido pudo contagiarle alguna enfermedad (casos de VIH) o si, por el contrario, la muerte fue producida por condicionantes genéticas (casos de prevención). Parece obvio que surge el derecho de la persona a conocer efectivamente si existen niveles de riesgo.

²⁶⁵ AAP de Madrid, 56-2005, de 3 de marzo de 2005, FJ: 3 (JUR 2005\108748). En este caso familiares pidieron al hospital, entregar la historia clínica y un informe explicativo de un pariente fallecido.

²⁶⁶ AAP de Pontevedra, 49-2006, de 9 de febrero de 2006, FJ:2 (JUR 2009\457410)

²⁶⁷ AAP de Islas Baleares, 88-2007, de 19 de junio de 2007, FJ: 3 (JUR 2007\311215)

Siendo así, no se traspasarán estos derechos a los herederos, y si el paciente no emitió concepto en cuanto la autorización de revelar sus datos clínicos, no deben ser expuestos a familiares o terceros no interesados.

2.7.4. Acceso a la historia clínica por parte de otros profesionales.

Tomando en consideración los fines descritos en páginas anteriores, la historia clínica, además de tener un fin asistencial, también podía ser utilizada para fines jurídicos, control de la calidad de atención y docencia e investigación. Sin embargo, esto no lo convierte en un documento de acceso público, al cual se puede recurrir, sin que sea realmente justificado su ingreso. En tal sentido, los centros sanitarios tienen la obligación de garantizar que sólo aquellos profesionales autorizados por la ley puedan utilizar la documentación clínica, aunque en el cumplimiento de esta obligación, tengan que desatender solicitudes, inclusive de personal con autoridad policial²⁶⁸.

Los inspectores médicos tendrían su acceso autorizado por ley, por ejemplo, pues realizan labores de control sobre el desarrollo de la actividad sanitaria, a efectos de conocer el desarrollo de la hospitalización, las prestaciones sanitarias, la valoración que se hace por equipos médicos e inclusive en temas múltiples incapacidades laborales de un trabajador. De igual forma, los inspectores farmacéuticos revisan las prescripciones farmacéuticas, a fin de controlar que las mismas sean acordes con el historial clínico del paciente.

Sobre este aspecto, sus trabajos requieren el acceso a la historia clínica, para poder obtener datos reales en cuanto a la ejecución de servicios en un determinado hospital, no siendo entonces una violación a la intimidad y a la protección de los datos del paciente, pues al ser profesionales están obligados a mantener la confidencialidad de los datos obtenidos.

²⁶⁸ SAP de Las Palmas, 431-2005, de 12 de septiembre de 2005, FJ: 4 (JUR 2005\215882)

Por otro lado, los médicos forenses en apoyo a la labor judicial también están autorizados para conocer las historias clínicas de los pacientes, pero esta facultad no escapa a la observancia de la ley. En este sentido, el médico forense sólo accederá a las historias clínicas, previa intervención del tribunal, mediante el respectivo oficio a la instancia sanitaria, de lo cual dicha instancia enviará el expediente, debidamente numerado, preferiblemente en original, siendo entonces el tribunal garante de su seguridad y reserva.

Así, la LOPD 15/1999 establece, en su art. 11.2.d, que no será necesario el consentimiento 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. (Ver capítulo 2.5.2.1.)

De contar con dicha autorización, el médico forense sólo puede acceder a la historia clínica, previo consentimiento del paciente y del médico, con las limitaciones que establece la ley, en especial las del secreto profesional.

2.8. De la cancelación de datos en la historia clínica.

La LOAP 41/2002 tampoco solucionó totalmente el tema de la cancelación de los datos, aun cuando era una necesidad evidente durante su redacción y aprobación. Efectivamente todo usuario/paciente tiene derecho a corregir la información que se tenga en cuanto a su persona, sin embargo, para hacerlo tendrá que apoyarse en otras normas, distintas a la LOAP 41/2002. En esta medida hay que entender que los datos personales que contienen todos los documentos e información que forma parte de la historia clínica, sin perjuicio de las previsiones legales anteriores, están amparados y protegidos muy

especialmente por la LOPD 15/1999²⁶⁹, especialmente en los temas de acceso, modificación de errores, cancelación etc.

En este orden de ideas, el art. 16.2 de la LOPD 15/1999 señala que serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente ley y, en particular, cuando tales datos resulten inexactos o incompletos. De esta manera, la historia clínica puede ser corregida en aquellos casos en los que la información contemplada no se ajuste a la realidad del paciente.

Ahora bien, para que la rectificación o cancelación se realice estará condicionada al cumplimiento de dos requisitos esenciales: primero, la acreditación de la procedencia de la rectificación o cancelación; y segundo, que el caso no se encuentre recogido en alguno de los supuestos establecido por el art. 33 del Real Decreto 1720/2007.

2.9. Conservación de la historia clínica.

Durante mucho tiempo el tema de la conservación de la historia clínica fue ampliamente discutido por la distintas comunidades autónomas, todo esto porque la LGS 14/1986 no señalaba el periodo exacto para su conservación. Por tal motivo, cada una aprobó de manera independiente, en sus respectivas legislaciones, los períodos de conservación que van, desde 20 años en Cataluña y 20 en el Reino de Navarra e indefinido²⁷⁰ en la ley de la Comunidad Autónoma de Galicia. Siendo así, reconocemos que la conservación completa de la historia clínica plantea problemas en relación con su manejo eficiente. Por eso se hace preciso expurgar y destruir la documentación que no se considera necesario guardar y conservar aquella que pueda tener valor en el futuro, bien para la

²⁶⁹Protección de datos personales para servicios sanitarios públicos, Edit. Agencia de Protección de datos de la Comunidad de Madrid, 2008, Madrid, p. 192

²⁷⁰ Aclaremos que hablamos de documentos relevantes, para los documentos no relevantes el plazo es menor.

asistencia al paciente, bien con fines judiciales o cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento.

La LOAP 41/2002 estableció que los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial. Este plazo ha sido criticado por DE LORENZO Y MONTERO, pues señala que la historia clínica es un medio de prueba fundamental en los procesos de exigencia de responsabilidad civil a los profesionales sanitarios y, si se insta la exigencia de responsabilidad, con amparo en la responsabilidad contractual del artículo 1.101 del Código Civil Español. El plazo de prescripción de la acción es de 15 años con lo que, si se ha destruido la historia clínica, se imposibilitará la prueba de falta de culpa o negligencia al profesional sanitario²⁷¹.

Este criterio, si bien ha dado un mínimo para la custodia de los documentos, no ha sido impedimento para que las comunidades autónomas, conserven sus propios plazos en cuanto a la conservación de este documento. Claro está, todos estos plazos son iguales o mayores que lo establecido en la propia ley general.

Ahora bien, cumplido el periodo de tiempo establecido por la LOAP 41/2002 se puede hacer expurgo en la documentación que conforma el historial clínico, conservando aquellos documentos de especial interés, para posibles consultas o procesos judiciales, lo cual igualmente critica DE LORENZO Y MONTERO²⁷² al señalar que las normas procesales,

²⁷¹ DE LORENZO Y MONTERO, Ricardo, "Propiedad y destino de los resultados de las investigaciones médicas, cuestiones referentes a la historia clínica", en MARTÍNEZ MORÁN, Narciso (Coord.), *Bioteología, derecho y dignidad humana*, Edit. Comares, Granada, 2003, p.307

²⁷² Vid supra

vinculantes en este tema, no incluyen en ningún momento términos o plazos, por lo que tal previsión está vacía de contenido en su origen.

2.10. La historia clínica informatizada.

La forma tradicional de elaborar una historia clínica es mediante el soporte en papel. Este método ha sido utilizado durante muchos años, con las consecuencias y problemas propios de almacenaje y disposición del documento. Al uso del papel para construir la historia clínica se le han señalado múltiples desventajas, entre las cuales se cuenta su manejo individual, el deterioro inminente de las mismas y el amplio espacio que requiere para su custodia.

El siguiente paso en la custodia de la información del paciente fue el de la formación de un archivo general en cada centro hospitalario²⁷³. Aunque funcionaban mejor, aun ocupan grandes superficies en los hospitales, dedicando bastantes recursos de personal al almacenamiento, custodia y distribución de las mismas, lo que supone aproximadamente un 0,5% anual del total del presupuesto hospitalario para disponer de una gestión adecuada de ella.²⁷⁴ La LOAP 41/2002 permite la utilización de “otros soportes” para la elaboración de las historias clínicas, siempre y cuando se resguarde la intimidad y la protección de los datos y la seguridad de los pacientes.

La digitalización de la información parece la solución más viable, pero su correcta distribución representa otro reto adicional en este cambio de paradigma, pues no sólo es

²⁷³MAZÓN RAMOS, Pilar y CARNICERO JIMÉNEZ DE AZCÁRATE, Javier, “La informatización de la documentación clínica: oportunidad de mejora de la práctica clínica y riesgos para la seguridad y confidencialidad (en línea)”, localizable en <http://www.seis.es/documentos/informes/secciones/adjunto1/1MazonCarnicero.pdf>

²⁷⁴CURIL HERRERO, Jesús y ESTÉVEZ LUCAS, Joaquín., Manual para la gestión sanitaria y de historia clínica hospitalaria, Editores Médico S.A., 2000, pág. 27.

procesar la información, sino lograr que ésta llegue a sus usuarios con la fidelidad y confidencialidad que exige la ley. Como todo sistema informático, también surge la obligación para el centro de proteger dichos expedientes, procediendo a cifrar los archivos. (entendiendo cifrar por “encriptar”), como un proceso mediante el cual se protege la información para que no pueda ser leída sin una clave. Esta forma de cifrar la información constituye una de las medidas de seguridad más usada para almacenar datos delicados de los hospitales, los cuales no deben ser accesibles a terceros.

Y es que los centros sanitarios deben reducir la vulnerabilidad en la seguridad de sus expedientes. Ya es por todos conocidos, dentro de los delitos informáticos, la irrupción ilegal de “expertos” en ficheros correspondientes a historias privadas. Los expertos, llamados también “piratas informáticos”, son personas que poseen amplio conocimiento acerca del funcionamiento interno de un sistema informático, en particular, sobre la seguridad de los mismos, lo que les permite ingresar a bases de datos y obtener, copiar y usar a su voluntad, información considerada como clasificada. En este sentido, se hizo patente la amenaza al derecho de la intimidad, cuando se publicó en una Web de Internet el libro del Dr. C. GUBBER y Mr. GONOD sobre la historia médica y política del que fue presidente de la República Francesa, FRANCOIS MITTERAND. El libro titulado “Le grand secret”, estuvo disponible en Internet sólo unos días, después que se prohibiera su venta en librerías, y violando los derechos de autor reconocidos en las leyes de propiedad intelectual.

En España, específicamente en la Comunidad Autónoma de la Rioja, ya los ciudadanos pueden consultar su historia clínica desde Internet. De acuerdo con Pedro Sanz²⁷⁵, presidente de dicha comunidad autónoma, los ciudadanos sólo tendrán que obtener su certificado digital o DNI electrónico para que puedan beneficiarse de este avance

²⁷⁵ Vid. Los riojanos pueden acceder a su historia clínica en Internet si disponen de certificado digital o DNI electrónico (en línea), Europapress.es, 25/11/2009, <http://www.europapress.es/la-rioja/noticia-riojanos-pueden-acceder-historia-clinica-internet-si-disponen-certificado-digital-dni-electronico-20091125131945.html>

tecnológico. Además, recalcó que La Rioja es la primera comunidad en poner este servicio en beneficio de la población y del personal sanitario.

La tendencia es clara. Si bien en estos momentos todavía existen centros sanitarios que utilizan un sistema en “soporte de papel normalizado”, no es menos cierto que pronto la evolución tecnológica también llegará en su totalidad a los archivos de los hospitales, lo que trae grandes ventajas, pero también nuevos retos para la intimidad del paciente. Al igual que se ha pasado de la imprenta, al CD Rom y de éste al sistema multimedia, las historias clínicas se renovarán en su contenido y forma, dando paso a una nueva generación de documentación electrónica.

Una de las características propias e inherentes a las tecnologías informáticas es su capacidad para recopilar, conservar y transmitir información de muy diverso signo e, incluso, también procesarla de modo tal que permita construir perfiles sociales de los ciudadanos²⁷⁶, siendo éste último elemento de mayor peligro para la intimidad del paciente. El derecho a la intimidad contenido en el art.18.1 CE no sólo preserva al individuo de la obtención ilegítima de datos de su esfera íntima por parte de terceros, sino también de la revelación, divulgación o publicidad no consentida de esos datos, y del uso o explotación de los mismos sin autorización de su titular.

Lo que el art. 18.1 CE garantiza es, por tanto, el secreto sobre la propia esfera de vida personal y, por tanto, veda a los terceros, particulares o poderes públicos, decidir sobre los contornos de la vida privada²⁷⁷. Otro reto implica la utilización de un DNI electrónico, el cual permite a los ciudadanos de un país europeo, por ejemplo, desplazarse virtualmente

²⁷⁶ SEMPERE NAVARRO, Antonio y SAN MARTÍN MAZZUCCONI, Carolina, “Intimidad del trabajador y registros informáticos”, en ÁLVAREZ CONDE, Enrique, *Revista Europea de Derechos Fundamentales*, Edit. Tirant lo Blanch, número 1, semestre 2003, p. 65

²⁷⁷ STC, 83-2002, de 22 de abril, FJ: 5 (RTC 2002\83)

entre diversos países de la unión, sin necesidad de trasladarse físicamente. Esta realidad también estaría pensada con los historiales clínicos y ya Bruselas plantea la posibilidad de regular esta materia²⁷⁸.

Notamos entonces que, además de proteger la salud del paciente, la elaboración de las historias clínicas conlleva diversos retos, desde el concepto de su titularidad, al acceso a la información y los nuevos medios tecnológicos para su constitución, teniendo como norte la protección de los derechos del paciente.

2.11. Naturaleza jurídica de la historia clínica y su validez probatoria en procesos judiciales.

Otro elemento que también se analiza en cuanto a la “propiedad” de la historia clínica es si al ser elaborada por un médico, en su consulta privada, podría ser considerada como un documento privado (expediente particular), o si, por el contrario, es un documento público (expediente administrativo), por ser elaborada por la autoridad sanitaria, mediante sus médicos y funcionarios.

Por un lado se señala que la historia clínica solamente puede ser considerada como documento privado, pues en ningún caso en su redacción se ejercen facultades de imperium. Sin embargo, también vale señalar que al ser elaborada por profesionales nombrados por el Estado (caso de médicos y hospitales públicos), se constituye en un documento público.

Pero, más allá de este debate, ¿puede la historia clínica dar “fe pública” de su contenido? Para NUÑEZ LAGOS, la fe pública es un concepto histórico, de matices místicos, que para la teoría general del Derecho no tiene otro significado que el de un grado o manera

²⁷⁸ Localizable en <http://www.20minutos.es/noticia/1497289/0/bruselas/dni-electronico/europa/>, fecha de consulta 4 de junio de 2012, 1:23 pm

de eficacia de ciertos hechos narrados en un texto documental, eficacia atribuida por la ley a una clase de documentos calificados de públicos²⁷⁹.

Para el Código Civil Español, en su artículo 1216, son documentos públicos los autorizados por un notario o empleado público competente, con las solemnidades requeridas por la ley. Luego entonces, es necesario distinguir si realmente la historia clínica, como prueba dentro del proceso, es irrefutable, y sus anotaciones tienen una presunción iuris et de iure o en cambio son iuris tantum.

La historia clínica, aunque sea confeccionada por médicos ligados por una relación jurídica de naturaleza pública con los servicios de salud, no tiene un carácter asimilable al de los papeles o libros privados, pero tampoco ostenta el carácter de documento público determinante de plenitud de prueba respecto de los extremos que dispone la ley...”²⁸⁰.

Sobre el particular, es importante destacar que el historial médico no hace fe por sí mismo de los datos que contiene, los cuales pueden ser contrastados con los demás medios probatorios, pues no tiene carácter intocable, ya que, a nuestra opinión, la historia no es más que el relato de un proceso médico, que puede o no ser verídico, y debe ser confrontado con los demás medios probatorios.

3. Resumen de ideas.

La historia clínica se constituye en un conjunto de documentos, valioso para el paciente, el personal médico y la Administración, pero todavía conserva aspectos que hacen complicado su manejo y, sobre todo, el reconocimiento de los derechos de las partes.

²⁷⁹ NUÑEZ LAGOS, Rafael, Perfiles de fe pública, Instituto Nacional de Estudios Jurídicos, Madrid, 1949, p. 5

²⁸⁰ STS, 84-2006, de 14 de febrero de 2006, FJ: 10 (RJ 2006\884)

El conflicto que aún persiste por el derecho de propiedad y de acceso no parece solucionarse tan solo con las leyes actuales que rigen la materia, aunque si hay un gran avance frente a la legislación vigente en 1986 hasta la fecha.

Dentro de los capítulos anteriores hemos mencionado reiteradamente dos derechos fundamentales que coexisten en este documento tan complejo. Por un lado el derecho a la protección de los datos y, más recientemente, el derecho a la intimidad, como un elemento muy vinculado a los datos de salud. Estos derechos no son los únicos que coexisten en este documento. Está también el derecho a la dignidad, con sus múltiples interpretaciones, el derecho a la salud y, como corolario de todos los anteriores, el derecho a la vida.

Cuando se habla de respeto al derecho a la intimidad en el contexto sanitario se incluyen aspectos tales como la confidencialidad de los registros médicos y la seguridad en la protección de la identificación del enfermo en las áreas de docencia, inclusive en aquellas investigaciones que se generen con el cuadro clínico que sufre el enfermo, en especial por la ética que debe guardarse ante las novedades biotecnológicas.

En la profesión médica es de sumo interés que exista un alto grado de empatía con el enfermo y sus necesidades. La ética es particularmente evidente, pues no queda duda que existe una desigualdad entre cuidadores y pacientes, siendo los últimos los más necesitados por la dependencia impuesta por la enfermedad.

Ya desde este punto se avanza que la intimidad es el conjunto de sentimientos y pensamientos que cada persona guarda en su interior como expresión de su identidad y cuya salvaguardia es un derecho. La pérdida de este valioso recurso del paciente puede acarrear cuadros de ansiedad y pérdidas de confianza en el personal sanitario que le atiende, lo que muy bien se puede traducir en peor condición de salud para el enfermo.

En este sentido, en el próximo capítulo la investigación analiza la gran relación que existe entre los datos de salud y la intimidad. Siendo así, se considera a la Intimidad, como un derecho de extraordinario valor, que está reconocido constitucionalmente, individualizado del resto de los derechos fundamentales y, además, protegido por múltiples instrumentos legales, nacionales e internacionales.

Cabe señalar que este capítulo se realiza sólo para destacar el gran vínculo que existe entre el derecho a la protección de los datos y la intimidad. En este sentido, la investigación hará un análisis a gran escala de este derecho fundamental, y sus características más importantes. Durante los primeros tres capítulos se menciona mucho el derecho a la intimidad pues, de una u otra manera, nutre la importancia que tiene para las personas, mantener en reserva su información.

CAPITULO 4

LA PROTECCIÓN DE LOS DATOS Y SU VINCULACIÓN CON LA INTIMIDAD

SUMARIO: 1. Aproximación al tema. 2. Concepto de intimidad. 2.1. Marco constitucional - derecho de intimidad del paciente. 2.2. Desarrollo de la protección constitucional. 2.3. Tipos de intimidad. 2.3.1. La intimidad corporal. 2.3.2. Otras formas de posible intromisión a la intimidad. 2.3.3. La intimidad económica. 3. De la revelación de secretos. 4. Protección de la intimidad en el código penal español. 5. Resumen de ideas.

1. Aproximación al tema.

Después de analizar los datos de salud y las características de la historia clínica, sus usos y el conflicto de propiedad que aún persiste entre los interesados, es importante continuar la investigación sobre otros aspectos vinculados a los datos y a la propia historia clínica.

De esta manera, se procede a analizar el derecho a la intimidad, por ser un relacionado directamente con la protección de los datos, como ya vimos en el capítulo 1. de esta investigación. Es un derecho innato al hombre y que ha sido considerado como uno de los derechos esenciales que emanan de la naturaleza humana, que se incluye dentro de los derechos naturales anteriores y, por tanto, superiores al reconocimiento que dan los derechos positivos.

El derecho a la intimidad personal ha sido probablemente el más repetidamente ignorado en el ámbito hospitalario, quizá por la novedad que existe en cuanto a los derechos reconocidos al paciente, aunque es verdad que en estos momentos se ha despertado una

mayor sensibilidad hacia el mismo, sobre todo por el conocimiento que existe sobre su existencia y capacidad de reclamación ante los Tribunales de justicia.

En este escenario, también cabe señalar el difícil recorrido jurídico que ha tenido este derecho en la legislación española y la protección total que alcanzó con la aprobación de la Constitución de 1978²⁸¹. En algunos casos, con el desarrollo de las leyes posteriores, aun se echaron en falta un desarrollo más profundo de los conceptos que se vinculan el derecho a la intimidad y que fue tarea de jueces y tribunales delimitar posteriormente.

Está claro, para profesionales sanitarios, que la relación clínica que soporta la atención de salud requiere de un ambiente de confianza, confidencia y lealtad. De ahí, que las normas de conducta obligan a preservar lo revelado en ese ambiente durante el ejercicio de la profesión.

De cualquier manera, como veremos más adelante, la intimidad involucra tantos aspectos que se hace muy complicado concretar una definición completa, ya que abarca áreas tan amplias como los sentimientos, los valores, las ideas políticas, las convicciones religiosas y otros. No obstante, esto no implica que la intimidad quede reducida a lo que podríamos denominar “núcleo duro” de la personalidad, que sería esa zona íntima que queda reservada a una persona o a un círculo restringido de personas.

En este marco conceptual, este trabajo pretende continuar la investigación analizando el derecho a la intimidad del paciente, precisamente el que se encuentra vinculado con los datos de salud y la manera en que la Constitución Española estableció un derecho perfectamente exigible por el paciente.

²⁸¹ CONCEPCIÓN HERNANDEZ, José Luis, Honor, intimidad e imagen, un análisis jurisprudencial de la LO. 1/1982, Bosh, 1996, p. 43

2. Concepto de intimidad.

Después de comentar las funciones y las características generales de la historia clínica, conviene avanzar hacia uno de los principales derechos que se protegen en este documento, me refiero a la intimidad y, en consecuencia, a la reserva de los datos del paciente, en función de su trato con la sociedad, pues no tendría sentido hablar de intimidad en la historia clínica en función de una persona aislada. La intimidad como muchos otros conceptos, posee una definición algo difusa o volátil²⁸², sobre todo por su novedad jurídica y la importancia que ha logrado en los últimos años. Precisamente porque el contenido de este derecho constitucional presenta unos rasgos imprecisos, posee una realidad intangible, es un concepto multiforme y variable, cuya extensión ha de determinarse atendiendo a las ideas y convicciones más generalizadas en la sociedad y en cada momento histórico. La manifestación probablemente más rotunda de esta concepción de la intimidad se encuentre en el art. 2.1 Ley 1/1982 que apela a los usos sociales como categoría delimitadora de la intimidad²⁸³. En otros casos, para definir el concepto de intimidad se propuso establecer determinados supuestos que se ajustaban a ataques o violaciones a este derecho, lo que no es aceptable, pues implica una técnica más propia de la tipificación de figuras delictivas penales y que puede dar lugar a que queden fuera de la protección de la intimidad casos no contemplados, siendo un sistema por demás imperfecto.

La cuestión de la imprecisión de concepto a lo mejor tendría cierta ventaja frente a la definición exacta, pues de estar definido el derecho a la intimidad, su campo de protección estaría limitado a ciertos extremos, y quedarían fuera de éste algunos casos que hoy son materia de protección por el derecho positivo.

²⁸² CREVILLÉN SÁNCHEZ, Clemente, Derechos de la personalidad. Honor, intimidad personal y familiar y propia imagen en la jurisprudencia, Doctrina y Jurisprudencia, 1996, p. 75

²⁸³ AAP de Córdoba, de 22 de julio de 1999, FJ: 3 (ARP 1999\2444)

El análisis del derecho a la intimidad puede situarse en dos sentidos en un extremo, con efecto negativo,²⁸⁴ en el que se define como el espacio reservado a los asuntos del sujeto frente a interferencias ajenas. En cuanto reserva, supone que hay un espacio de actividad que es exclusivo y que no puede ser conocido por otros sujetos, por otro lado, el extremo con efecto de control, como la oposición al conocimiento y manejo de la información del titular, especialmente en bases de datos, sin su consentimiento. En esto no solo nos referimos a los particulares, sino también a la no intervención por parte del Estado²⁸⁵ en los asuntos que conciernen al individuo. Esta segunda dimensión de la intimidad, conocida como libertad informática o habeas data, encuentra su apoyo en el artículo 18.4 CE, en el que se dispone que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. De esa proclamación se deriva un poder de acción del titular para exigir que determinados datos personales no sean conocidos²⁸⁶. Resulta evidente que en el aspecto de control, el derecho a la intimidad es la base fundamental para su defensa en los tribunales, sobre todo en el caso de las historias clínicas, ya que no solamente es la posibilidad de mantener la vida privada (datos médicos) en reserva, sino la facultad de prohibir, amparados

²⁸⁴ MUNAR B, Pedro A (Et al), Enciclopedia Jurídica Básica, Vol. III, Edit. Civitas S. A, año 1995, p.3725

²⁸⁵ En el derecho Norteamericano existen varios casos en los que el Tribunal Supremo de los Estados Unidos ha declarado ilegal leyes Estatales, por ejemplo, *Griswold vs. Connecticut*, 381 US 479 (1965), en el que se estima que una ley del Estado de Connecticut que castigaba el uso de anticonceptivos en el seno del matrimonio implicaba una injerencia injustificada en la intimidad conyugal, en la medida que el Estado no puede interferir en decisiones sobre el uso de anticonceptivos de una pareja casada. También, *Loving vs. Virginia* 388 U.S.1 (1967), en el que el Tribunal Supremo declaró inconstitucional una ley que penalizaba el matrimonio interracial, indicando que los Estados no pueden interferir hasta el punto en la decisión individual del cónyuge acerca de con quién casarse. Y por último, *Eisenstadt vs. Baird* 405 U.S. 438 (1972), extendiendo la argumentación del caso *Griswold* para anular una ley que prohibía la distribución de anticonceptivos a personas no casadas.

²⁸⁶ GONZÁLEZ RUS, Juan, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en COBO DEL ROSAL, Manuel (Coord.), Derecho Penal Español – Parte Especial, Edit. Dykinson SL, 2004, Madrid, p. 343

en el derecho, que otros, sin el debido permiso, puedan acceder a ellos o darlos a conocer por cualquier medio, sean estos estudios, publicaciones, etc.

El término intimidad proviene del griego *éntos*, que significa dentro, del que deriva en latín el adverbio de igual significado *intus*, y de ahí el comparativo interior (más dentro que) y el superlativo *íntimus* (lo más dentro)²⁸⁷. La intimidad surge como una necesidad social. La primacía de lo privado frente a lo público, no se debe a la existencia de una motivación humana fundamental, y sí como una reacción ante la pérdida de control de lo que nos rodea, es en esencia una conducta²⁸⁸. Para la Real Academia de la Lengua Española, la intimidad es la zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia²⁸⁹. De lo anterior, se comparte lo señalado por GIL HERNANDEZ cuando dice que esta definición es meramente unívoca, de modo que el derecho a la intimidad, *privacy*, o *reservatezza* del individuo se proyecta en una doble vertiente: de libertad de vivir cada uno su propia vida conforme a sus gustos o preferencias, sin imposiciones uniformadoras del grupo social, y de vivirla en sociedad, de manera que el goce de esa libertad no vulnere los iguales derechos o intereses de los demás.²⁹⁰

Por otro lado, en un tono un poco más restringido, HERRAN la define como una reserva interna, más allá de su condición grupal, pues, aunque el ser humano es social por naturaleza, pese a ello, no deja de sentir la necesidad de realizar una vida interior, ajena a las relaciones que mantiene con otros individuos y que le permite identificarse como ser

²⁸⁷ SÁNCHEZ CARO, Jesús y SÁNCHEZ CARO, Javier, *El médico y la intimidad*, Edit. Díaz de Santos, 2001, Madrid, p.3

²⁸⁸ REBOLLO DELGADO, Lucrecio, "El Derecho a la intimidad", en TORRES DEL MORAL, Antonio (Dir.), *Libertades informativas*, Colex, 2009, p. 243

²⁸⁹ Real Academia de la Lengua Española, vigésima edición, versión electrónica.

²⁹⁰ GIL HERNÁNDEZ, Ángel, "Protección de la intimidad corporal: aspectos penales y procesales", en *Revista General de Derecho*, Valencia, Julio – Agosto, 1996, p. 7951

humano ²⁹¹ y es que no hay que olvidar que el ser humano se desenvuelve en tres espacios principales: el público, el privado y el íntimo. De otro modo, tal como señala CONCEPCIÓN RODRÍGUEZ, “todas estas definiciones implican un concepto de autonomía que muchas veces también es usado para describir este derecho, junto con el de soledad o aislamiento, que se traduce en el derecho a ser dejado solo y tranquilo”.²⁹²

Sin querer restarle valor, aclaramos que en el espacio público no hay mayores problemas, ya que no hay tantos intereses que resguardar, en este medio los datos son básicamente del conocimiento colectivo. No obstante, son los ámbitos privados e íntimos los que más requieren de nuestro interés, sobre todo por la relevancia que alcanzan para el paciente.

Para CRUZ, se puede advertir en castellano al menos una doble dialéctica en el término “íntimo” la primera, entre exterior/interior (estímulos íntimo), parecida a la de superficial/profundo; y la segunda, la de público/privado (en defensa de lo íntimo), por ejemplo “no publicar cosas tan íntimas”. Esta última, que también podría ser expresada como individuo/comunidad política, no es sólo una distinción ideológica sino uno de los presupuestos de la política y tiene una gran trascendencia para el derecho²⁹³. En definitiva, el derecho subjetivo a la vida privada se constituye básicamente en un derecho subjetivo a estar libre de intromisiones tanto por parte de los poderes públicos como por terceros (incluidos los propios hospitales), que entraña restricciones respecto a la recogida,

²⁹¹ HERRÁN O. Ana Isabel, El Derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales, Edit. Dykinson, 2002, p. 19

²⁹² CONCEPCIÓN HERNANDEZ, José Luis, Honor, intimidad e imagen, un análisis jurisprudencial de la LO. 1/1982, Op. Cit., pp. 41 y 42

²⁹³ CRUZ, Juan, El éxtasis de la intimidad. Ontología del amor humano en Tomas de Aquino, Madrid, Edit. Rialp, 1999; p. 16

comunicación, uso y difusión de información de carácter personal dando lugar a lo que en la doctrina alemana se ha denominada “una autodeterminación informativa”²⁹⁴.

En este sentido, el Estado debe proteger a los ciudadanos e inhibirse de conocer datos privados de los particulares (pacientes), salvo casos muy excepcionales y, además, garantizar mediante la promulgación de leyes que protejan al individuo de que otros violen su intimidad. De no hacer esto último, estaría desconociendo la garantía constitucional, con las consecuencias correspondientes a cada caso. Ya desde la propia Constitución Española se brindan los medios a los afectados, específicamente en el art. 53.2 de la CE, que señala que cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el art. 14 y la Sección 1ª. del Capítulo II ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional.

De esta manera, el derecho a la intimidad ha modificado la forma de proteger otros derechos, su reconocimiento a nivel constitucional ha desplegado otras modalidades de cobertura legal. Para ÁLVAREZ – CIENFUEGOS SUÁREZ, puede ser considerado como el derecho fundamental del siglo XXI, ya que si no hay intimidad no habrá nada²⁹⁵. Desde otra perspectiva, la intimidad se define bien como el ámbito en el que cada persona encuentra la posibilidad de desarrollar su personalidad, también como la manifestación de la personalidad individual o familiar cuyo conocimiento cada persona reserva para sí o sobre la que ejerce control. Por eso se dice que comprende las circunstancias o hechos que una persona desea

²⁹⁴ CONTRERAS MAZARÍO, José M., “Derecho a la intimidad, pruebas biomédicas y relaciones laborales. Especial referencia a la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas”, en *Derechos y Libertades*, Revista del Instituto Bartolomé de las Casas, Universidad Carlos III, Año V, Julio/Diciembre, 2000, número 9, p. 209

²⁹⁵ ÁLVAREZ – CIENFUEGOS SUÁREZ, José María, Aspectos jurídicos y protección de datos sanitarios, Resumen de la II Jornada Madrileña de Admisión y Documentación Médica. Madrid, Fundación Hospital de Alcorcón, 20 de mayo de 1999; p.59.

que sólo sean conocidos por ella o por un limitado número de otras personas²⁹⁶. Para un análisis más práctico, consideramos correcta la idea de los círculos concéntricos, tipo esfera, que reflejan el nivel de relación entre el individuo y la sociedad, mientras más se cierra el círculo, más privada es la zona, el espacio más cercano al individuo es la intimidad.

A su vez, al concepto de intimidad se le asocia comúnmente con la privacidad, pero es un hecho que son términos generalmente disímiles en esencia, si bien es cierto que podría decirse que la intimidad está amparada dentro de la privacidad, por ser esta última más amplia y abarcadora que la anterior, no es menos cierto que ambas gozan de una “esfera propia” de existencia. Dentro de la intimidad podemos contar, por ejemplo, los pensamientos, las tendencias políticas, los datos de salud y la orientación sexual. Al contrario, la privacidad como aspecto más amplio que hasta se comparte con la sociedad, tendría como ejemplo el lugar de trabajo, la dirección de residencia, las asociaciones a las que se pertenece y/o el grado académico, etc. Esta diferencia es importante para el Derecho y, en ese sentido, según MUÑOZ CONDE, el derecho a la intimidad se configura como uno de los derechos de la personalidad más sutiles y más difíciles de delimitar y proteger por el Derecho Penal²⁹⁷.

Sobre la privacidad, BEJAR la considera como elemento más amplio del sujeto, sería la práctica de la soledad buscada²⁹⁸, el escape temporal de unas exigencias y cargas de una interacción que se vive como excesiva u opresiva. La privacidad no sería tanto un

²⁹⁶ ATSJ de la Comunidad Valenciana, 10/1999, de 18 de febrero de 1999, FJ: 2 (ARP 1999\1040)

²⁹⁷ MUÑOZ CONDE, Francisco, Derecho Penal – Parte Especial, Edit. Tirant lo Blanch, Valencia, 2004, p. 256

²⁹⁸ En cuanto al concepto de Soledad, autores como FROSSINI, Vittorio, “La Tutela de la Privacidad: de la libertad informática al bien jurídico informático”, Revista del Colegio de Abogados de Buenos Aires, núm. 2, 1989, p.86, defienden que es un concepto ya superado y que en su lugar la libertad informática sustituye al antiguo Right to Privacy, pues el primero ha adquirido un carácter positivo, que no solo abarca la esfera de la privacidad, sino también la facultad de acceso, de control, de rectificación y hasta de cancelación de los datos personales insertos en un banco de datos.

instinto como una necesidad socialmente creada²⁹⁹. En definitiva, para este autor, la intimidad sería lo más interno e inexpresable del hombre, que apunta a una zona sagrada, aquello que nos podría causar alegría o vergüenza y que simplemente no queremos compartir con otros sujetos de la sociedad.

Ahora la intimidad no es sólo, como derecho fundamental, un derecho al ocultamiento de circunstancias personales, sino un derecho a la no divulgación ilegal de los datos, dado que configura una forma del derecho a la libre realización de la personalidad³⁰⁰. Es precisamente esta protección de datos la que ha sido normada por la legislación española mediante su ordenamiento jurídico. En efecto, el derecho a la intimidad personal garantizado por la Constitución tiene un contenido más amplio que el relativo a la intimidad corporal, habida cuenta de que “el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art.10.1 CE), integra un ámbito propio y reservado frente a la acción y el conocimiento de los demás, referido preferentemente a la esfera, estrictamente personal, de la vida privada o de lo íntimo.”³⁰¹ Para VIVES ANTÓN, desde una concepción estrictamente jurídica, la dignidad de la persona, como sujeto de derecho, constituye la esencia misma del honor y determina su contenido³⁰². Es justo señalar que cada derecho conlleva una obligación y así como exigimos el respeto de nuestra intimidad, tenemos la obligación de respetar también la intimidad ajena. Pero esta obligación es la que usualmente se desconoce y a la sociedad le cuesta mucho cumplir, debido a los patrones culturales en los que se vive.

²⁹⁹ BEJAR, Helena, *El ámbito íntimo. privacidad, individualismo y modernidad*, Edit. Alianza, Madrid, 1995, p. 44

³⁰⁰ SAP de las Islas Baleares, 11/2009, 11 de febrero de 2009, FJ: 4 (ARP 2009\351)

³⁰¹ FERNÁNDEZ COSTALES, Javier, “Intimidad de la persona y confidencialidad de los datos en el marco de la vigilancia de la salud. El respeto a los derechos del trabajador en los reconocimientos médicos”, en *Revista Derecho y Salud*, volumen 16, Nº1, enero - junio 2008, p.96.

³⁰² VIVES ANTÓN, Tomás, “Delitos contra el Honor”, en *Derecho Penal – Parte Especial 2da. Edición*, VIVES ANTÓN, T.; ORTS BERENGUER, E.; CARBONELL MATEU, J.; GONZÁLEZ CUSSAC, J. y MARTÍNEZ – BUJUAN PÉREZ, C., Edit. Tirant Lo Blanch, 2008, p. 314

Tal vez el morbo y el deseo “natural” de conocer qué sucede a nuestro alrededor hace que este derecho a la privacidad y la intimidad, de acuerdo a su propio ámbito de competencia, sea ignorado y constantemente amenazado, pues en ocasiones, para los temas de salud, que son de los que se ocupa esta investigación, son los propios profesionales sanitarios quienes incumplen con el deber de secreto, facilitando información de carácter confidencial, y no necesariamente “de importancia pública”, a los medios de comunicación para lograr notoriedad o beneficios económicos. Inclusive, es alarmante cómo la propia sociedad ve esta conducta como algo normal y hay poca reclamación ante la violación de estos derechos que tanto han costado proteger para lograr una sana convivencia.

Es común ver en programas de televisión o radio “entrevistas”, cómo profesionales de la salud hablan de la vida privada de sus pacientes y referirse a detalles que claramente pertenecen a su esfera privada. Tal actitud no puede ampararse en las excepciones que da la ley, por ejemplo, para temas relevantes de interés social cuya fuente sea veraz (art. 20.1 d de la CE), por lo que hay que resaltar que la libertad de expresión dispone de un campo de acción delimitado por la ausencia de expresiones indudablemente injuriosas, que resulten innecesarias para la exposición de las mismas y que no contravengan otros valores constitucionales o derechos fundamentales³⁰³. Aunque la sociedad lo tolera, es un derecho que los individuos “cotizan” comercialmente, debido a que, como señala ALONSO DE ESCAMILLA, la intimidad es un bien jurídico protegido de naturaleza subjetiva, por lo que la delimitación y el contenido de la misma en el caso concreto pertenecen al sujeto pasivo, quién será en buena medida el que determine el ataque a la misma³⁰⁴.

³⁰³ SAP de Sevilla, 404-2007, de 25 de septiembre de 2007, FJ: 4 (AC 2008\1979)

³⁰⁴ ALONSO DE ESCAMILLA, Avelina, “Delitos contra la intimidad, el derecho a la propia Imagen y la inviolabilidad del domicilio”, en LAMARCA PÉREZ, Carmen (Coord.), Derecho Penal Parte Especial, Edit. Colex, Madrid, 2008, p. 182

Por otro lado, siguiendo con los conceptos generales, la palabra “privacy” adaptada al castellano privacidad, tiene un contexto diferente, inclusive desde su raíz etimológica, en si privacy, proviene del latín privatus (privo, privus), que significa separado aislado, peculiar o personal, y a diferencia de “intimidad”, del griego Indus adoptado por el latín intimus, la privacy hace referencia al estado de la persona frente a su semejantes (público/privado), no a su estado interno (ideas y sentimientos).

Aunque en la práctica parece que el uso diario de ambos términos es confuso, también es obligatorio señalar que el “derecho a la privacidad” o “Right to privacy”, proviene del sistema anglosajón, y se constituye, efectivamente, según el legislador, en una esfera más amplia dentro de la vida de la persona. Su defensa está garantizada en el derecho, aunque no se concibe como el núcleo esencial y básico del sujeto. De esto podemos sacar como primera conclusión que no todo lo privado es íntimo, pero todo lo íntimo sí es privado.

Por tal motivo, se comparte lo expresado por ORTS BERENGUER Y GONZÁLES CUSSAC, cuando señala que se confunden los términos y que la privacidad es el bien jurídico específico del delito establecido en el art. 171 del Código Penal Español. A su criterio, son muchos los ámbitos de la vida privada de las personas que pueden estar registrados en los objetos materiales del delito..., y que, en consecuencia, pueden ser invadidos de forma ilícita; ámbitos relacionados con la vida amorosa o sexual, con la salud, con las creencias, con las situación económica, etc.³⁰⁵

Ahora bien, como antecedentes, resaltamos que los primeros en definir este “derecho a la privacidad” fueron SAMUEL WARREN Y LOUIS BRANDEIS en un famoso artículo publicado en la Harvard Law Review el año 1890, en el que se debatía el derecho de las personas a que sus asuntos privados no pudieran ser divulgados y por lo tanto conocidos por

³⁰⁵ ORTS BERENGUER, Enrique y GONZÁLES CUSSAC, José, Compendio de derecho penal (Parte general y especial), Edit. Tirant lo Blanch, Valencia, 2004, p.490

otras personas, sin el consentimiento del titular (artículo que se elaboró como respuesta a la creciente influencia de la prensa en la opinión pública). El título del artículo es por demás significativo: “the Right to Privacy”. WARREN Y BRANDEIS tuvieron conciencia de que estaban escribiendo un nuevo derecho humano, un derecho privado, subjetivo y personalísimo.³⁰⁶ El “nuevo” derecho fundamental a la intimidad/privacidad es la prueba más concreta de que los derechos humanos no son estáticos, ni sus categorías inamovibles; su reconocimiento y protección responde a la evolución de la sociedad y al pensamiento que defiende la autodeterminación de las personas y su capacidad de reservar para sí mismo aspectos ulteriores, no divulgables ni traspasables a terceros, salvo exista consentimiento expreso de su titular.

La evolución del derecho positivo va desarrollando cada vez más esta protección a la intimidad, especialmente frente a la informática y sus efectos en la nueva sociedad moderna. Conviene hacer una importante precisión al respecto, según AGUSTINA SANLLEHI. Si bien en el derecho norteamericano se define el right to privacy en función de la existencia de una “expectativa razonable de privacidad”, no ocurre lo mismo en el ordenamiento jurídico español. La explicación es muy sencilla: mientras que en la cultura jurídica norteamericana se configura el derecho a la privacidad como una mera propiedad del individuo, de naturaleza absolutamente disponible, recibiendo así un tratamiento jurídico equivalente al derecho de la propiedad. En el ordenamiento jurídico español y en el ámbito comunitario, la intimidad no es una propiedad y se establecen unos mínimos indispensables o, mejor dicho, se contemplan supuestos en los que se considera que el consentimiento o la libre aceptación de la persona en la cesión de su intimidad o la renuncia se considera nula ex art.1.3 LO 1/1982, pues no reúne las necesarias condiciones de validez en atención a las circunstancias concurrentes.³⁰⁷ Claro está, esto se aplicará para los casos de renuncia total a

³⁰⁶ SÁNCHEZ CARAZO, Carmen, La intimidad y el secreto médico, Edit. Díaz de Santos, 2000, prólogo, p. XV.

³⁰⁷ AGUSTINA SANLLEHI, José R., El delito de descubrimiento y revelación de secretos en su aplicación al control del correo electrónico del trabajador, Edit. La Ley, 2009, pp. 96 – 97.

la intimidad, tema que es prohibido por la legislación, lo que no impide la libertad propia del individuo a consentir el manejo de su información de acuerdo a condiciones previamente pactadas.

Como consecuencia de las diferencias señaladas en párrafos anteriores, parecería que la intimidad y la privacidad son términos excluyentes entre sí. Sin embargo, esto no es del todo cierto, pues constituyen dos aspectos complementarios e interdependientes de la existencia humana, quiere ello decir que una protección completa de la persona frente a las agresiones de las tecnologías de la información únicamente se alcanzará a través de la tutela de ambas esferas de actuación del sujeto.³⁰⁸ También es complicado separar la intimidad y la privacidad, pues son conceptos tan subjetivos que es cada individuo quien decide cuáles son sus límites exactos. Así, hay personas que prefieren exponer sus problemas de salud ante el público sin mayor reparo y hay otros que prefieren reservárselos estrictamente para sí mismos. Lo que no puede negarse es que el patrimonio que comprende la intimidad personal es extremadamente amplio y variado, sin que puedan sentarse reglas generales, ni catálogos enunciativos de la misma, pero sí hacer referencia a todos aquellos datos biológicos o espirituales o caracterológicos que componen el ser de una persona³⁰⁹. VIVES ANTON señala que el problema es, ciertamente, arduo; pero tal vez pueda encontrarse solución apelando a la idea de que, si bien la dignidad es única e igual para todos, las diferentes posiciones y situaciones de los individuos comportan que el respeto a esa dignidad y los ataques a la misma requieran una determinación circunstancial³¹⁰.

Entre tanto, el derecho a la intimidad no está por encima de todo y puede ser limitado, especialmente cuando el individuo entra en contacto con legítimos intereses de terceros, legalmente protegidos, desde una función pública que lo convierte en garante de

³⁰⁸ HERRAN O. ANA, Op. Cit., p.44

³⁰⁹ SAP de Málaga, 11-2004, de 5 de marzo de 2004, FJ: 5 (AC 2004\464)

³¹⁰ VIVES ANTÓN, Tomás, Op. Cit., p. 316

derechos de terceros.³¹¹ De esta manera, los Tribunales han dejado claro que, por ejemplo, los espacios de trabajo no son considerados áreas privadas, siendo posible su control mediante sistemas de vigilancia sin que esto afecte la intimidad del trabajador. Asimismo, los funcionarios públicos que en el ejercicio de sus funciones, conocen datos protegidos de terceros no pueden alegar que el manejo de tales datos se produce dentro del ámbito de la esfera reservada al desarrollo y realización de su personalidad, pues este límite de su privacidad surge directamente del derecho de múltiples ciudadanos que pueden verse afectados por una extensión del derecho de los funcionarios que impida todo control de una tarea que afecta de manera muy sensible a derechos de terceros.³¹²

2.1. Marco Constitucional - Derecho de intimidad del paciente.

Está claro que los pacientes, además del respeto a su salud, tienen derecho a mantener esta condición en forma confidencial. Este derecho puede basarse en el art. 18.1 de la Constitución Española, que garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. La intimidad, como derecho constitucional, es de reciente reconocimiento, lo que lo hace novedoso, pues durante muchos años no fue considerado como tal. En su lugar sólo existían modalidades de protección a la intimidad (inviolabilidad del domicilio y la correspondencia), siendo estos los más usuales en las constituciones de la época, especialmente en América Latina, de ahí que algunos autores como FARIÑAS, reconocen que el derecho a la intimidad es único desde su concepción, pero múltiple y relativo en sus manifestaciones³¹³. Ahora bien, MARTÍN SANJUÁN señala que, aunque el reconocimiento expreso en los textos constitucionales es muy reciente, lo cierto es que su idea originaria aparece ya en algunos de los textos clásicos, y en el más paradigmático de ellos, por su carácter internacional y amplio consenso: la Declaración Universal de los

³¹¹ SAP de Cádiz, 10 -2006, 17 de enero de 2006, FJ: 1 (JUR 2006\172776)

³¹² STS, 725-2004, 11 de junio de 2004, FJ: 1 (RJ 2004\5625)

³¹³ FARIÑAS M., Luis, El derecho a la intimidad, Madrid, Edit. Trivium, 1983, p.327

Derechos del hombre 1948, en la que se afirma que nadie será objeto de intromisiones arbitrarias en su vida privada, su domicilio o su correspondencia, ni de atentados contra su honor y reputación³¹⁴. La controversia que existe, según la autora, surge en la falta de consenso en la delimitación de su contenido (la pregunta “qué es”), y la determinación de cuál es su fundamento (la pregunta “porqué”)

Para CUESTA PASTOR, “en los últimos tiempos, estamos asistiendo a la irrupción en nuestra sociedad de nuevas tecnologías, nuevas formas científicas, que están trastocando importantes planos de la misma”³¹⁵. Por eso, proteger la intimidad ahora es más necesario, sobre todo por los avances de la tecnología y los medios masivos de comunicación, que han puesto en alerta y peligro la dignidad de las personas. No es de extrañar que mediante el uso de las herramientas de la informática, se pueda afectar gravemente el honor o la dignidad de una persona, con las consecuencias morales que esto acarrea para la víctima, ya que la deshonra puede hacerles desmerecer aprecio y respeto del público que les rodea.

³¹⁴ MARTÍN SANJUÁN, Cristina, “Cribado genético: el conflicto entre el derecho a la información y el derecho a la intimidad”, en MARTÍNEZ MORÁN, Narciso (Coord.), Biotecnología, Derecho y Dignidad Humana, Edit. Comares, Granada, 2003, p. 316

³¹⁵ CUESTA PASTOR, Pablo, “Los mecanismos de identificación y su uso en el proceso penal: interrogantes a propósito de la huella de ADN”, en ROMEO CASABONA, Carlos (Editor), Bases de datos de perfiles de ADN y criminalidad, Edit. Comares S.L., Granada, 2002, p.75. El autor destaca cómo ha impactado el dato genético en la investigación de los delitos, tanto como lo hizo en su momento la huella dactilar, se apoya en el carácter individual y único del dato genético, que salvo casos muy especiales, no se repite en varios sujetos a la vez. De igual forma, advierte que este tipo de datos no solo sirven para identificar a un sujeto, sino que también expone su “esencia”, lo que hace necesario un procedimiento muy especial, para no violar elementos esenciales de la intimidad. En una conclusión importante, dice que no existe duda de que el desarrollo científico no puede ser limitado, dado los grandes beneficios que arroja para la investigación, en áreas como la criminalística, penalística (sic) y de política criminal, pero esto no puede permitir que se cometan abusos con los derechos fundamentales.

Del mismo modo, SÁNCHEZ PATRÓN dice que “los progresos llevados a cabo en el ámbito de la biomedicina aumentan el interés de los terceros en obtener información sobre dichos datos biomédicos y, por otro lado, la facilidad y la profusión con las que la información es difundida en nuestros días incrementa el recelo de los pacientes a que sus datos personales pueden ser divulgados sin que se haya obtenido el consentimiento pertinente”³¹⁶. Para este autor, aunque los datos de salud pueden ser almacenados en forma manual y automatizada, son este último grupo los que tienen un riesgo elevado sobre la confidencialidad de los datos, criterio que se comparte, si evaluamos la gran cantidad de información que se puede compilar en espacios de memoria tan pequeños. La portabilidad de los mismos, casi supera a la imaginación actual y en pequeños dispositivos, fijos y móviles, se pueden trasportar bibliotecas enteras de información.

El art.18.1 tiene como eje básico los derechos de la personalidad³¹⁷ y precisamente el rango constitucional garantiza su prevalencia por encima de cualquiera disposición que le sea contraria. Nadie está autorizado a obtener, ceder, y hasta sacar provecho con los datos privados de otros. Inclusive el derecho a la libertad de expresión, comúnmente en conflicto con el derecho a la intimidad y establecido en el art. 20 de la CE, encuentra sus límites en el art. 18.1. Ahora bien, tal como lo mencionamos anteriormente, conviene aclarar que aunque el derecho a la intimidad es fundamental, no es ilimitado, por lo que existen casos en los que se puede suspender temporalmente su cumplimiento, con base

³¹⁶ SÁNCHEZ PATRÓN, José M, “El régimen jurídico europeo aplicable a la confidencialidad de los datos relativos a la salud de las personas”, en TOMÁS – VALIENTE L, Carmen (Coord.), La salud intimidad y libertades personales, Valencia, 2006, p. 210

³¹⁷ Desde una concepción lusnaturalista, los derechos a la personalidad conciben y reconocen al ser humano como depositario de ciertas garantías innatas, por su propia naturaleza, que no necesitan la tutela de la ley para su existencia, para BUSTOS PUECHE, José Enrique, en su obra Manual sobre bienes y derechos de la personalidad, año 1997, Edit. Dykinson, sólo son derechos de la personalidad, los de vida, integridad física, honor e intimidad. La imagen, puede considerarse una sub especie o manifestación concreta de la intimidad, pp. 46 – 47.

a la regla de la proporcionalidad³¹⁸, la cual obliga a que, de darse una suspensión a los derechos fundamentales de una persona, la resolución que así lo determine, deberá motivarse, pues sólo tal fundamentación permitirá que se aprecie, en primer lugar, por el afectado y que se pueda controlar, después, la razón que justificó, a juicio del órgano judicial, el sacrificio del derecho fundamental.³¹⁹ Sobre el derecho a la libertad de expresión, solo se admite como excepción, a la protección de la dignidad, cuando lleva consigo la libertad de información, no el de opinión, de modo y manera que la protección constitucional se extiende únicamente a que la información sea veraz, sin romper la necesaria objetividad informativa, de modo que por quien informa, no se actúa con mala fe ni con culpa profesional grave³²⁰. Por tal razón, toda resolución que limite o restrinja el ejercicio de un derecho fundamental ha de estar motivada añadiéndose que las medidas limitadoras habrán de ser necesarias para conseguir el fin perseguido³²¹.

Exponer ante la palestra pública la condición de salud de un particular, sin su consentimiento, acarrea serias consecuencias, en especial se le expone a los posibles prejuicios de la sociedad. Independientemente de que se trate de una persona conocida o no, temas como el padecimiento del VIH, la práctica de abortos o sufrir una enfermedad mental, provocan un inmediato rechazo entre las personas. En este sentido, el art. 20.1 d. CE, efectivamente protege el derecho a comunicar o recibir libremente información veraz

³¹⁸ El principio de la proporcionalidad en sentido estricto no es más que la ponderación entre los intereses en juego, para que la limitación de los derechos no tenga cabida en todo caso, sino sólo frente a adecuadas exigencias del interés estatal y, en todo caso, siempre que se hayan intentado, o no quepan, otros medios que impliquen evitar una lesión en los derechos del individuo, así como que la medida por la que se produce la limitación de aquellos sea también adecuada. En estos casos, la regla también exige una identidad, ya que la medida aplicada solo pueda darse (en materia policial), cuando existan fundadas sospechas sobre la comisión de un delito, siendo la medida la que menos lesivo al derecho fundamental.

³¹⁹ STC, 37-1989, de 15 de febrero, FJ: 8 (RTC 1989\37)

³²⁰ STC, 127-2003, de 30 de junio, FJ: 4 (RTC 2003\127)

³²¹ STC, 13-1985, de 31 de enero, FJ: 2 (RTC 1985\13)

por cualquier medio de difusión, pero esto no es óbice para que todos los temas sean objeto de comunicación o información al público. Aclaremos que los conceptos “personaje público y personajes con notoriedad pública” son diferentes entre sí. Evidentemente, los primeros son aquellos que ejercen el poder público/estatal y, debido al cargo que ostentan, están sometidos a la vigilancia y control de la población debido al carácter “representativo” que se les concedió, por tanto se encuadran dentro de lo permitido por el art. 20 1.d de la CE. Por contrario, las personas con notoriedad pública son aquellas cuya profesión implica un contacto diario con los medios de comunicación o aquellas que por una situación inesperada son reconocidos ante la sociedad. En ambos casos, esta calidad en la persona no impide que tengan derecho a su intimidad y estén obligadas a ser expuestas en su intimidad, más allá de lo que conscientemente hayan aceptado.

En si, los derechos a la imagen y a la intimidad personal y familiar reconocidos en el art. 18.1 de la CE aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la dignidad de la persona³²², que reconoce el art. 10 de la CE y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario para mantener una calidad mínima de la vida humana.³²³ La dignidad humana podrá ser también, como algunos sugieren, un recipiente que puede contener las cosas más heterogéneas... es sabido que el concepto y el problema de la dignidad humana es más amplio que el de los derechos, pero en ella encontramos “la

³²² La dignidad humana no es sólo un derecho que se reconoce al hombre y a la mujer, sino el fundamento de los derechos que se conceden al ser humano, su expresión hace referencia al valor intrínseco e inalienable que posee la humanidad, independientemente de los diferentes grupos que existen. Cfr., STARCK, Christian, en “La dignidad del hombre como garantía constitucional, en especial en el derecho Alemán”, publicado por FERNANDEZ S., Francisco (coord.), Dignidad de la persona, derechos fundamentales, justicia constitucional, Edit. Dykinson S.L., 2008, p. 241. Las diferentes teorías filosóficas y corrientes ideológicas comprenden y definen la dignidad de forma diferente. Hay un concepto de Dignidad, Cristiano, humanista – ilustrado, marxista, teórico – sistemático y del Behaviorismo,

³²³ STC, 231-1988, de 2 de diciembre, FJ: 3 (RTC 1988\231)

síntesis”, de todos los demás derechos: es la contratación de la unidad indiscutible de todos los hombres, de quienes puede predicarse que son el “concretum universale”³²⁴.

Ahora sobran los programas televisivos especialistas en indagar en la vida privada de particulares, para desvelar sus datos íntimos o en el peor de los casos se toman tragedias humanas y familiares para explotar la audiencia en un medio determinado. Para José Joaquín Gallardo, Decano del Colegio de Abogados de Sevilla, en el caso de Marta del Castillo³²⁵, “algunas cadenas de televisión están usando su imagen e intimidad con fines claramente comerciales, que la ley prohíbe, creando productos televisivos en torno a su persona que sobrepasan con mucho el derecho a la información”.³²⁶ En este caso se critica la utilización claramente comercial de los derechos personales de la víctima, que la ley de protección al honor prohíbe expresamente, sin embargo por el morbo malsano del público se obtuvo ganancias de una tragedia familiar.

Sobre estos derechos (honor, intimidad e imagen), se cuestionó si eran autónomos o si, por el contrario, pertenecían a un solo derecho, el llamado “derecho a la privacidad”. En este sentido, resuelve el Tribunal Constitucional diciendo que para abordar

³²⁴ BERTOLINO, Rinaldo, “La cultura moderna de los derechos y la dignidad del hombre”, en Revista de Derechos y Libertades – Revista del Instituto Bartolomé de las Casas, Año IV, enero 1999, número 7, p. 135. y 136. El autor también señala que la dignidad humana podrá ser también un recipiente que puede contener las cosas más heterogéneas, pero hay una circunstancia sobre la que existe ya pleno acuerdo: el reconocimiento de que la persona es autónoma, autolegisladora; que es el nuevo y objetivo baricentro de nuestro tiempo, que la capacidad de todo hombre en cuanto persona es, en su dimensión institucional, mínima y fundamental, “constitutiva de sentido”

³²⁵ El caso Marta del Castillo trata sobre el secuestro y asesinato de una adolescente en Sevilla - España, en el cual su novio (homicida confeso), engañó a la policía señalando falsos sitios en los que supuestamente arrojó el cadáver. Este tema ha motivado revuelo principalmente por el trato dado por los medios de comunicación a los familiares y personas allegadas a la joven asesinada.

³²⁶ Tal cual aparece publicado en el diario electrónico, el mundo.es, de fecha 19 de abril de 2009, localizable en el enlace http://www.elmundo.es/elmundo/2009/04/19/andalucia_sevilla/1240164032.html

tal cuestión debe recordarse que los derechos al honor, a la intimidad personal y familiar y a la propia imagen son derechos autónomos. De este modo, al tener cada uno de ellos su propia sustantividad, la apreciación de la vulneración de uno no conlleva necesariamente la vulneración de los demás.³²⁷ Por tal motivo, existen claras diferencias en cuanto al nivel de afectación y defensa de cada derecho per se. En cuanto al derecho al honor, este puede ser reclamado tanto por personas físicas como jurídicas, teniendo efectos inclusive posterior a la muerte o disolución, respectivamente. Sin embargo, en el derecho a la intimidad, los Tribunales sólo han reconocido este derecho a las personas físicas³²⁸ y no a las personas jurídicas, pues un sector de la doctrina considera que la tutela de datos o informaciones de tipo societario o empresarial en sentido estricto no entran, prima facie en la “ratio” de tutela del precepto en cuanto que este tipo de información ya está tutelada en el ámbito de los delitos relativos al mercado (art. 278 y siguientes).³²⁹

Para las personas físicas, “el derecho a la intimidad se extingue con su muerte, ya que una vez fallecido el titular de esos derechos y extinguida su personalidad, se extingue también su derecho. Según determinación el art. 32 Código Civil Español, “la personalidad civil se extingue por la muerte de las personas”, lógicamente desaparece también el mismo objeto de la protección constitucional que está encaminada a garantizar un ámbito vital reservado que con la muerte deviene inexistente”.³³⁰ Ante este criterio de la doctrina queda algo de recelo, sobre todo por el valor que tiene “la memoria” de la persona que ha fallecido y aunque entendemos que no podría reclamarse un derecho a la intimidad del difunto, nos parece que su recuerdo por lo menos debe quedar amparado en la ley. Por tal razón, reconforta cuando en sentencia del Tribunal Constitucional, se abre paréntesis a su línea doctrinal y se reconoce que, aunque existe derecho a la información por parte de los medios

³²⁷ STC, 156-2001, de 2 de julio, FJ: 2 (RTC 2001\156)

³²⁸ STC, 137-1985, de 17 de octubre, FJ: 2 (RTC 1985\137)

³²⁹ SAP, 72-2002, Sevilla, de 15 de febrero de 2002, FJ: 1 (ARP 2002\253)

³³⁰ AAP Córdoba, de 22 de julio 1999, FJ: 3 (ARP 1999\2444)

de comunicación, la misma, al margen de su veracidad o falsedad, puede lesionar de manera ilegítima el honor y la intimidad de una persona fallecida, puesto que, en el juicio que se hizo sobre su personalidad, cuyo resultado global de descalificación moral, social y profesional es innegable, se incluyen expresiones y afirmaciones que exceden del ámbito en el que debe entenderse prevalente el derecho de información. (...) tanto más cuanto que se trate de una persona fallecida, cuya memoria, de acuerdo con el sentimiento social prevalente, merece el mayor respeto.³³¹

De igual forma, en cuanto a los parientes, el Tribunal Constitucional ha reconocido su derecho a la protección de la intimidad familiar, en aquellos casos en los que se trastoque la intimidad de un allegado fallecido³³². En este sentido, podría ampliarse la facultad de reclamo de los familiares en aquellas ocasiones en los que se les afecte indirectamente, pero eso será sólo si hay afectación “familiar”, de lo contrario no se podría presentar queja o demanda “en nombre de”. El Tribunal Constitucional también ha reconocido que el derecho personalísimo de un particular puede a afectar la intimidad de otros, como en el caso de familiares que demandaron la emisión de imágenes de un padre y esposo muerto. Se trata, pues, de imágenes de las que, con seguridad, puede inferirse, dentro de las pautas de nuestra cultura, que inciden negativamente, causando dolor y angustia en los familiares cercanos del fallecido, no sólo por la situación que reflejan en ese momento, sino también puestas en relación con el hecho de que las heridas y lesiones que allí se muestran causaron, en muy breve plazo, la muerte del torero. No cabe pues dudar de que las imágenes en cuestión, y según lo arriba dicho inciden en la intimidad personal y familiar de la hoy recurrente, entonces esposa, y hoy viuda, del desaparecido señor R.³³³

³³¹ STC, 172 ,de 12 de noviembre de 1990, FJ: 4 (RTC 1990\172)

³³² STC, 231-1988, de 2 de diciembre, FJ: 4 (RTC 1988\231)

³³³ STC, 231-1988, de 2 de diciembre, FJ: 6 (RTC 1988\231)

2.2. Desarrollo de la protección constitucional.

Con la aprobación de la Constitución Española de 1978, se aprobó posteriormente 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, como una norma general y después, de forma más específica se aprobó la LOPD. 15/1999. En resumen, ambos ordenamientos tienen como objetivo principal garantizar las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Empezando con la Ley Orgánica 1/1982, su campo de aplicación se refiere más a la esfera civil, pero ya desde su artículo 7 establece que se consideran intromisiones ilegítimas la revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.

Sobre esta norma, el Tribunal Constitucional, sin prescindir de ella por completo, no se ha sentido especialmente vinculado por sus concretos postulados a la hora de proceder a la interpretación constitucional de estos derechos³³⁴. Pensamos que su fundamento podría estar en la crítica que advierte BUSTOS, al decir que existe una superfluidad de la

³³⁴ PARDO FALCÓN, Javier, “Los Derechos al honor, a la intimidad personal y familiar y a la propia imagen”, en CASAS BAAMONDE, María y RODRÍGUEZ PIÑERO Y BRAVO –FERRER, Miguel, Comentarios a la Constitución Española, año 2008, p. 415. El autor señala este comportamiento como lógico, ya que ni la citada Ley (1/1982), muy breve, pretendía una regulación pormenorizada de los mismos, ni tampoco tal cosa resultaba conveniente si tenemos en cuenta que, a diferencias de otros derechos fundamentales, los derechos de la personalidad no son en sentido estricto derechos de configuración legal, lo que los hace jurisdiccionalmente muy asequibles y especialmente idóneos para la aplicación directa que se refiere del art. 53.1 CE. Consecuentemente, con ello resulta, pues, que la Ley 1/1982, lejos de proporcionar algún tipo de definición de los derechos que regula, se limite a establecer que su protección civil “quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí o su familia”.

construcción, pues desde el momento en que las Constituciones ya reconocen derechos fundamentales, los relativos a los bienes de la personalidad, sería una duplicidad innecesaria la protección jurídico – civil³³⁵. En lo particular, no estamos de acuerdo con esta crítica, pues los principios enunciados en la Constituciones no se ejecutan automáticamente ante el ciudadano, siendo necesario el desarrollo que haga la ley para su efectivo cumplimiento. Es más, muchos de los artículos de la constitución son meramente programáticos, indicando qué es lo que quiere lograr el derecho, pero no dice cómo debe hacerse. Es allí donde radica el verdadero valor de las leyes orgánicas, pues toman el principio constitucional y lo operacionalizan de forma que puede cumplirse con los objetivos propuestos en las normas constitucionales.

2.3. Tipos de intimidad.

Ya que nos referimos a la asistencia sanitaria, es importante distinguir que este derecho a la intimidad y a la privacidad plantea su aplicación en distintas áreas, la corporal (intimidad física), la de la confidencialidad (intimidad informacional), y la de la toma de decisiones (intimidad decisional).³³⁶ Por esto, la legislación nacional y hasta el derecho internacional han tratado de proteger, de forma integral, la intimidad de la persona. Así la LGS 14/1986, la LOAP 41/2002 y la LOPD 15/1999 protegen directamente la confidencialidad de la información.

Y es que el simple ingreso del paciente en el hospital conlleva una limitación de su intimidad en esos tres factores, desde el momento de su llegada es sometido al interrogatorio propio para de la anamnesis, mencionada en el capítulo anterior. De ser necesaria la hospitalización, será sometido a constantes controles corporales, por lo que aquí

³³⁵ BUSTOS PUECHE, Op. Cit., p.38.

³³⁶ EGUSQUIZA BALMASEDA, Ma. Ángeles, Protección de datos: intimidad y salud, Edit. Arazandi, S.A., 2009, p.27.

también verá como su intimidad será “compartida”, con otros pacientes y por ultimo hasta tendrá que decidir, si conviene o no, facilitar su información en pro de la investigación científica.

Es evidente que en un hospital el paciente accede a compartir esa intimidad con el equipo médico, en aras de obtener un bien superior (lograr un diagnóstico correcto y un tratamiento adecuado), pero esta intimidad “limitada” no puede disminuir el trato que merece como persona. Uno de los errores que más se cometen dentro de los hospitales es cosificar al paciente y tratarlo como un simple expediente o estadística, pues aunque esté enfermo posee tanta dignidad como una persona sana, simplemente que por su condición de paciente denota cierta dependencia y necesidad de mayor apoyo.

2.3.1. La intimidad corporal.

La intimidad corporal puede entenderse desde varios aspectos, sin embargo es importante señalar que somos seres humanos, con cuerpo y pensamiento, por tanto reaccionamos ante nuestra expresividad, sobre cómo nos manifestamos y cómo nos comprometemos ante el resto de la comunidad, en especial, por la identidad que asumimos y cómo podría ser afectada. Este pensamiento incesante es el que motiva el pudor o la vergüenza que sentimos ante la opinión pública y por eso reclamamos el derecho a la intimidad corporal, especialmente si hablamos de intervenciones médicas. En la medida que la persona toma consciencia de si misma y que su interioridad se desarrolla, más reclama la intimidad corporal. Este hábito del pudor también está en condiciones de crecer, por eso es que los niños o infantes al no verse sometidos al juicio de la sociedad, tienen menos limitaciones en este aspecto.

Ahora bien, para defender la intimidad corporal también es necesario una madurez interior y hasta una evolución social. En los primeros años de convivencia, la

intimidad corporal no era un tema que realmente importara al ser humano, el cuerpo se cubría más por una necesidad de protección ante las inclemencias del clima que por una cuestión de pudor. Igualmente, en la medicina la intimidad corporal era y es, hasta cierta medida, condicionada a la interpretación y decisión de los facultativos, quienes disponían lo que más conviene al paciente, en ejercicio del principio paternalista.

Hay que reconocer que existe un sensible cambio en cuanto a la decisión del tratamiento médico, pero aún persiste la poca o nula “intimidad del cuerpo”, mientras el paciente se encuentra recluido en hospital. Decimos esto, pues a veces ni siquiera se le garantiza un espacio privado. Las habitaciones regularmente se comparten y qué decir de las prendas de vestir que casi no reservan nada a la imaginación de las personas que rodean al paciente. Los hospitales varían dependiendo del país y, dentro de éste, a la región a la que pertenecen. Es más común ver cómo en países menos desarrollados, considerados del tercer mundo, los pacientes no tienen ni siquiera una cama en la cual descansar, en el mejor de los casos hasta la comparten con otro paciente, en ocasiones esperan en los pasillos, mientras esperan la asistencia sanitaria. ¿Dónde queda la intimidad y la dignidad de este paciente, que en su necesidad de auxilio tiene que soportar condiciones que rayan en la poca consideración humana?

Sobre este tema, El Tribunal Constitucional³³⁷ ha reiterado que la Constitución garantiza la intimidad personal (art. 18.1), de la que forma parte la intimidad corporal, de principio inmune, en las relaciones jurídico-públicas que ahora importan, frente a toda indagación o pesquisa que sobre el cuerpo quisiera imponerse contra la voluntad de la persona, cuyo sentimiento de pudor queda así protegido por el ordenamiento, en tanto responda a estimaciones y criterios arraigados en la cultura de la comunidad. Asimismo aclara que esta afirmación de principio requiere, claro está, algunas matizaciones. La primera de ellas, implícita en lo ya dicho, es la de que el ámbito de intimidad corporal

³³⁷ STC, 37-1989, de 15 de febrero, FJ: 7 (RTC 1989\37)

constitucionalmente protegido no es coextenso con el de la realidad física del cuerpo humano, porque no es una Entidad física, sino cultural y determinada, en consecuencia, por el criterio dominante en nuestra cultura sobre el recato corporal, de tal modo que no pueden entenderse como intromisiones forzadas en la intimidad aquellas actuaciones que, por las partes del cuerpo humano sobre las que se operan o por los instrumentos mediante las que se realizan, no constituyen, según un sano criterio, violación del pudor o recato de la persona. La segunda es la de que, aun tratándose ya de actuaciones que afectan al ámbito protegido, es también cierto que la intimidad personal puede llegar a ceder, en ciertos casos y en cualquiera de sus diversas expresiones, ante exigencias públicas, pues no es éste un derecho de carácter absoluto, pese a que la Constitución, al enunciarlo, no haya establecido de modo expreso, la reserva de intervención judicial que figura en las normas declarativas de la inviolabilidad del domicilio o del secreto de las comunicaciones (apartados 2 y 3 del mismo art. 18).

Siguiendo este planteamiento, la LOAP 41/2002, mediante su artículo 8.1, protege la intimidad corporal, pues dice que toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el art. 4, haya valorado las opciones propias del caso. Luego entonces, cualquier procedimiento, en especial los invasivos en su cuerpo, deberán ser previamente consentidos por el paciente, con base a la información completa que debe ser proporcionada por el personal sanitario.

Por otro lado, también hay que destacar que esta intimidad corporal tampoco es un blindaje excepcional para el sujeto, pues en casos de comisión de delitos, y bajo ciertos criterios, es posible obligar a la persona a exámenes médicos. Tal afectación del ámbito de la intimidad es posible sólo por decisión judicial que habrá de prever que su ejecución sea

respetuosa con la dignidad de la persona y no constitutiva, atendidas las circunstancias del caso, de trato degradante alguno.³³⁸

Se incluyen en estos supuestos los lavados estomacales obligatorios para las personas que presuntamente trasiegan drogas dentro de su anatomía, a los que previamente se les somete a revisión médica y exámenes de rayos x. Asimismo, las pruebas de alcoholemia en caso de conductores que sean sorprendidos conduciendo bajos los efectos del alcohol e inclusive los exámenes de consumo de drogas, para deslindar responsabilidades penales.

Por otro lado, este derecho a la intimidad corporal no puede oponerse como una barrera para lograr la impunidad, en los casos de actos que violenten el derecho. En este sentido, para los casos de pruebas médicas tendentes a identificar la paternidad de un sujeto, no se considera que tal acción viole la intimidad corporal del paciente, pues dicha prueba está legalmente aprobada para estos casos y está además acordada con la autoridad judicial.

También, aunque no se considera una supuesta intromisión física, pero si psicológica, hay que analizar los casos de prácticas de pruebas periciales conducentes a determinar la capacidad intelectual y mental del inculpado. Aquí, aunque puede decirse que obligar al sindicado a realizar la prueba podría ir en contra de su autodeterminación, también es preciso destacar que este tipo de pruebas no son invasivas en el cuerpo y tampoco limitan en el sospechoso el control sobre sus facultades intelectuales y de conciencia; por el contrario, son reconocimientos pacíficos, altamente aceptados por los grupos de derechos humanos.

³³⁸ STC, 37-1989, de 15 de febrero, FJ: 7 (RTC 1989\37)

Se aprecia, además, que en este tipo de reconocimientos, no se intenta doblegar la voluntad del paciente y lograr su declaración de culpabilidad, más bien se busca determinar si existen rasgos de su personalidad que influyen en sus decisiones o manera de comportarse y a la vez lo hagan responsable o no ante la ley por sus actos.

En otro caso, tampoco se considera violación a la intimidad que los privados de libertad compartan una misma celda, pues dicha convivencia no implica una renuncia a los elementos más esenciales del derecho a la intimidad y bien podría considerarse como un caso de “vida interior”. Sin embargo, debido al grado de sujeción que existe en los sistemas penitenciarios, es normal que los cacheos sean parte de la rutina, y podría pensarse aquí en una violación a la intimidad corporal. Pero este tipo de actividad no se realiza sin fundamento, por el contrario, está debidamente regulada y se constituye en una simple exploración corporal para evitar la comisión de delitos.

Es más, la propia reglamentación interna de las prisiones hace viable imponer la desnudez del cuerpo del detenido, en razón de la realización de requisas por la posible existencia de material ilegal dentro del recinto carcelario. Esta requisita, que en el mejor de los casos debe ser comunicada formalmente al recluso antes de ser practicada, debe hacerse atendiendo los principios fundamentales de los Derechos Humanos.

Ahora bien, lo que si podría ir en contra de este derecho a la intimidad y la dignidad en las prisiones, sería el maltrato, las vejaciones u órdenes que impliquen, además de la desnudez del cuerpo, las burlas y amenazas que, acompañadas de actividades de ejercicio físico, ubiquen al detenido en un claro nivel de inferioridad.

2.3.2. Otras formas de posible intromisión a la intimidad.

Con motivo de las graves actividades terroristas, que tienen su punto de partida en los atentados de las torres gemelas ubicadas en New York, Estados Unidos de Norteamérica, se reforzó el control en los aeropuertos y se han instalado mayores inspecciones de seguridad para los viajeros, con énfasis en los artículos que llevan y si representan o no un peligro para el viaje. En esto, se impone un análisis a los casos de revisiones de equipajes, de los cuales, si se realizan de forma desordenada y agresiva, podrían poner al descubierto aspectos de la vida privada de un particular, que no tiene porqué ser desvelados.

En si, los enseres en general estarían protegidos dentro del derecho a la intimidad de la persona, pues algunos de ellos podrían exponer sus preferencias ideológicas o sexuales. Sin embargo, aquella revisión de equipajes que se realice con el conocimiento de su dueño y conforme a reglas preestablecidas, se consideraría dentro del marco autorizado por la ley.

En igual medida, siempre y cuando la ley lo autorice, se puede afectar la intimidad de la correspondencia y del domicilio, en aquellos casos en los que corresponda a una medida necesaria para preservar la pacífica convivencia.

Esta revisión debe ser practicada siempre por el personal idóneo para estas labores. Y el ejemplo es perfectamente aplicable a hospitales, en los que el personal médico podría revisar el equipaje que acompaña al paciente, a fin de determinar cuáles son las variables que pudieron influir en la actual condición del enfermo, y hasta determinar con base en estas pruebas, tratamiento o procedimientos tendientes a su cura.

2.3.3. La intimidación económica.

En este aspecto se abarca la información que recaban las autoridades tributarias y en razón de las obligaciones de las personas a pagar impuestos ante el fisco. En igual medida, con base en los recientes ataques terroristas, se ha abierto el debate de si el Estado tiene derecho a acceder a las cuentas bancarias de los ciudadanos y tener el control sobre el movimiento de los fondos de dinero.

Ahora, el contribuyente debe justificar con mayor detalle todas las operaciones bancarias que realice, en especial aquellas que correspondan al ingreso y salida de dinero en las cuentas bancarias nacionales y extranjeras.

Contrario a esto, se defiende la afectación del derecho a la intimidad, señalan que la inspección ilimitada y total de las cuentas corrientes y de sus antecedentes, tiene efectos peligrosos, ya que se autorizaría para entrar sin limitación alguna en la vida privada del contribuyente, en forma tal que no es ya que afecte en modo más o menos directo a su derecho a la intimidad, sino que, en realidad, invade su contenido esencial, pues lo hace prácticamente desaparecer.

Por otro lado, se considera que “las certificaciones de movimiento de las cuentas no viola, en sí, el secreto profesional, ni la intimidad, puesto que en ellas sólo aparece la causa genérica de cada operación y no el contenido concreto de la relación subyacente”. Es cierto que se permite investigar los saldos y movimientos de las cuentas, así como los documentos y demás antecedentes relativos a los mismos y que en los casos que se proceda a la investigación se puede exigir la entera colaboración en la recolección de los datos, antecedentes y circunstancias que, referentes al sujeto investigado, existan en cualquiera de sus oficinas. Sin embargo, esta facultad no es abierta, está condicionada la autorización de los órganos competente, un propósito definido y hasta extremos claros, sobre qué

documentos se deben requerir o investigar, en igual forma, quiénes accedan a esta información están obligados a callar lo que saben.

La justificación más importante de lo anterior es que, de no hacerse, se facilitaría el fraude fiscal de algunas personas al poder camuflar sus ingresos y su patrimonio al amparo de sus relaciones profesionales con los clientes. Además, que no se podría identificar el depósito o retiro de dinero que serviría para financiar actividades delictivas, por lo que la intromisión en las cuentas bancarias estaría justificada, si con eso se puede garantizar una convivencia pacífica.

3. De la revelación de secretos.

Conocer la información, en algunos casos, implica la obligación de callar, más si se tuvo acceso a los datos producto del ejercicio de un cargo o la realización de funciones que llevan aparejadas el permiso de conocer expedientes privados.

Para la Real Academia de la Lengua Española, el secreto es la cosa que cuidadosamente se tiene reservada y oculta³³⁹. Esta definición no ofrece una guía exacta para este término, en su lugar desarrolla las conductas y sanciones atribuibles a las personas que sin estar autorizados accedan a “los secretos” de otras personas. El secreto opera como un derecho fundamental-medio o sea, en la calidad de dispositivo de protección de ciertos procesos comunicativos que en la práctica social son el cauce de transmisión de datos comprendidos en el ámbito del derecho fundamental/fin que es la intimidad personal³⁴⁰.

MUÑOZ CONDE dice que el carácter de secreto de un hecho lo determina la propia voluntad del interesado o titular que tiene derecho a que no se conozcan hechos

³³⁹ Diccionario de la Real Academia de la Lengua Española, versión electrónica, XXII Edición.

³⁴⁰ AAP de Madrid, 413-2007, 29 de junio de 2007, FJ: 1 (JUR 2007\309543)

relativos a su intimidad más allá del estricto círculo de personas que por razón de su cargo tienen que conocerlo³⁴¹. Y, rizando el rizo, JUANES PECES señala que cuando lo descubierto es irrelevante desde el punto de vista social, no existe delito porque lo decisivo a estos efectos es la vulneración del bien jurídico protegido, que no se produce cuando lo que se descubre o revela carece de relevancia desde la perspectiva material del derecho protegido que, recordemos, es la privacidad de la persona³⁴².

Asimismo, ARROYO ZAPATERO señala que, “aunque en el artículo 197.1 del Código Penal Español se sancionan las conductas encaminadas a descubrir los secretos o vulnerar la intimidad, que atentan contra el derecho de exclusión. Pese a esta dualidad, el término secreto no tiene un contenido independiente, sino que ha de interpretarse a la luz del bien jurídico intimidad”³⁴³. Sin embargo, SEGRELLES DE ARENZA, también destaca que una solución acorde a los diferentes principios por los que se rigen el Derecho Penal y el Civil consiste en clasificar los grupos de casos de agresiones a la intimidad (grabación de imágenes y demás), diferenciando entre lugares privados o públicos, y éstos a su vez, en cerrados o abiertos. En el extremo más restrictivo se encuentra el lugar privado y además cerrado, cuya protección es evidente que corresponde al Derecho penal³⁴⁴

Para la Audiencia Provincial de Madrid³⁴⁵, lo que se garantiza constitucionalmente es un derecho al secreto, a ser desconocido, a que los demás no sepan

³⁴¹ MUÑOZ CONDE, Francisco, Violación de secretos. Uso indebido de Información privilegiada, Junta de Andalucía Consejería de Gobernación y Justicia, Instituto Andaluz de Administración Pública. p. 6.

³⁴²JUANES PECES, Ángel, “Comentarios a los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en CONDE – PUMPIDO TOURÓN, Rogelio (Dir.), Comentarios al Código Penal, Edit. Bosh, Barcelona, 2007, p. 1542

³⁴³ ARROYO ZAPATERO, Luis (Et al), Comentarios al Código Penal, Op. Cit, p. 472

³⁴⁴ SEGRELLES DE ARENZA, Iñigo, “Delitos contra la Intimidad”, COBO DEL ROSAL, Manuel (Dir.), Compendio de Derecho Penal Español, Edit. Marcial Pons, 2000, p. 273

³⁴⁵ AAP de Madrid, 116-2008, 5 de junio de 2008, FJ: 2 (ARP 2008\679)

qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio, resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio y pudiendo imponer a terceros su voluntad de no dar a conocer dicha información o prohibir su difusión no consentida, lo que ha de encontrar sus límites en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos. De igual forma, el concepto de secreto, que aparece en el artículo 18.3 de la CE, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales³⁴⁶.

Dado que analizamos el tema del secreto en esta parte, es necesario señalar que para SEGRELLES DE ARENAZA la estructura del secreto se compone del objeto, que puede ser un hecho, conducta, pensamiento, intención, objeto, producto, procedimiento, etc.; Conocimiento, en el sentido de noción, datos, información sobre el objeto, carácter oculto, el conocimiento no ha de estar alcance de todos; elemento subjetivo, sólo cuando hay voluntad de que el conocimiento permanezca oculto se podrá hablar de secreto; elemento objetivo (interés), conforme a un criterio objetivo de valoración, el conocimiento ha de tener suficiente entidad para ser digno de protección. En otras palabras, tiene que concurrir un interés, que generalmente será un bien jurídico, para mantener oculto el conocimiento y sujetos, al menos uno en posesión del conocimiento (activo) y otro que carezca de él (pasivo)³⁴⁷.

³⁴⁶ SÁNCHEZ MELGAR, Julián (Coord.), Código Penal – Comentarios y Jurisprudencia, Edit. Sepín, 2004, p. 1090

³⁴⁷ SEGRELLES DE ARENAZA, Iñigo, “Delitos contra la intimidad”, en COBO DEL ROSAL, Manuel (Dir.), Op. Cit., pp. 270 y 271

Sobre el secreto, REBOLLO VARGAS³⁴⁸ se ha planteado algunos supuestos, desde la teoría de la voluntad (*willenstheorie*), que define al secreto como una consecuencia de un acto subjetivo, que tiene origen en la propia voluntad del sujeto, quien le otorga a una determinada información o conocimiento el carácter de secreto y la teoría del interés (*interessentheorie*), cuyo fundamento es que existen hechos que por su propia naturaleza son objetivamente calificadas como secreto; y esto es con independencia a la prohibición, limitación o manifestación de una o más voluntades.

Sobre el particular, el autor no está de acuerdo con que existan hechos que por su naturaleza sean considerados como secretos; es más, señala que existen hechos que están tipificados por la norma, siendo objeto de protección en consecuencia. En tal sentido me sumo a este planteamiento, pues no considero que los hechos “nacen con categorías de secreto”, más bien considero que son los actos humanos y su interpretación los que determinan si un hecho o conocimiento debe quedar en la reserva y conocimiento de pocos o ningunos.

Lo interesante en estas dos teorías es que en la primera pareciera un acto impositivo en el que la simple voluntad del sujeto le da la categoría de secreto al hecho, desde su percepción muy particular. Evidentemente, estaríamos frente una calificación de la cosa, desde la “óptica que se mire”, sin que realmente pudiésemos constatar si tiene o no relevancia jurídico penal. Por otro lado, en cuanto a la teoría del interés, solo se basan en el origen “natural” del secreto, para darle un valor superior, aquí tampoco podríamos constatar si al derecho penal realmente le interesa este “secreto”, como para generar su protección. En ambos sentidos se concentran más en lo que consideran, desde sus propias perspectivas, como secreto, sin verificar lo más importante, que es identificar qué lo que se busca proteger con el secreto.

³⁴⁸ REBOLLO VARGAS, Rafael, *La Revelación de Secretos e informaciones por funcionario Público*, Edit. Cedecs, 1996, pp. 138 – 139

Y es que este tema es fundamental, pues el secreto en sí no parece un bien jurídico autónomo, sino que está ligado a otros intereses que pretende proteger. Si hablamos entonces del secreto de estado, se busca proteger la Administración Pública o, en lo que interesa a nuestro trabajo, sobre el secreto de las historias clínicas, a la intimidad y dignidad de las personas. Así coincidimos con MORALES PRATS, cuando señala que el secreto es exclusivamente un elemento o técnica jurídica instrumental, en si mismo vacío de contenido, que puede estar al servicio y tener por objeto múltiples intereses o bienes jurídicos ..., la referencia a la intimidad, auténtico y único bien jurídico tutelado hubiera bastado³⁴⁹. Los tribunales, por otro lado, han manifestado que la simple obtención de documentos³⁵⁰ no constituye una revelación de secretos, más bien se toma en consideración si la información que en ellos se establece forma parte de la intimidad de la persona o si su apoderamiento realmente devela un secreto. Sobre este planteamiento lo que es relevante es el contenido y no el documento, DIAZ REVORIO discrepa y dice que no solo el contenido de la comunicación es importante, sino también el soporte de la misma, y las circunstancias que lo rodean³⁵¹.

Ahora bien, es prohibido por la norma revelar los datos o la conversación sostenida entre dos personas, pero no es prohibido revelar la propia conversación. "Quien graba una conversación de otros atenta, independientemente de otra consideración, al derecho reconocido en el art. 18.3 de la Constitución Española; por el contrario, quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado. Si se impusiera un deber genérico de secreto a cada uno de los interlocutores o de los corresponsables "ex" art. 18.3 CE, se terminaría vaciando de sentido, en buena parte de su alcance normativo, a la protección de la esfera íntima personal "ex" art.

³⁴⁹ MORALES PRATS, Fermín, Op. Cit., p. 411

³⁵⁰ SAP de Teruel, 4-2002, de 6 de mayo de 2002, FJ: 2 (ARP 2002\471)

³⁵¹ DIAZ REVORIO, Javier, "El derecho fundamental al secreto de las comunicaciones", en Revista de Derecho PUC, Edit. Fondo, N° 59, 2007, p. 162

18.1, garantía esta que, a contrario, no universaliza el deber de secreto, permitiendo reconocerlo sólo al objeto de preservar dicha intimidad (dimensión material del secreto). Los resultados a que podría llevar tal imposición indiscriminada de una obligación de silencio al interlocutor son, como se comprende, del todo irrazonables y contradictorios, en definitiva, con la misma posibilidad de los procesos de libre comunicación...”.³⁵²

En esencia, el secreto es comunicado a un limitado grupo de personas, cada una con la obligación de no transmitir a terceros el contenido de la información, pero surgen claras contradicciones cuando el “secreto”, constituye un hecho notorio que ha salido del dominio de las personas a quien se había confiado inicialmente, son los llamados rumores no confirmados, o secretos a voces. Aunque, por otro lado, en la Sentencia 114/1984 se afirma, en efecto, que no hay secreto para aquel a quien la comunicación se dirige ni implica contravención de lo dispuesto en el art. 18.3 de la Constitución la retención por cualquier medio del contenido del mensaje,³⁵³ pero también hay que reconocer que no sólo hay ámbitos recónditos de la intimidad personal en lo concerniente al secreto de las comunicaciones, sino también lo que se ha denominado autodeterminación informativa, entendida como derecho de toda persona a determinar por sí misma, quién puede grabar su palabra y ante quién puede ser reproducida su voz.

4. Protección de la intimidad en el Código Penal español.

Igual que en la Constitución Española, el Código Penal Español tiene una reciente historia en cuanto a la protección al derecho a la intimidad, configurado como lo es en la actualidad³⁵⁴, es más los atentados contra este bien jurídico, no fueron objeto de estudio en

³⁵² SAP de Madrid, 115-1999, de 15 de abril de 1999, FJ: 2 (ARP 1999\1762)

³⁵³ STC, 114-1984, 29 de noviembre de 1984 FJ: 7 (RTC 1984\114)

³⁵⁴ OLMO FERNANDEZ – DELGADO, Leopoldo, “Estudio histórico del delito de descubrimiento y revelación de secretos”, en Revista Aranzadi de Derecho y Proceso Penal, Edit. Aranzadi, Año 2009 – 2, número 22, p. 111. El autor destaca que esta protección es novedosa por dos razones, porque está asociada al Estado Moderno y

profundidad por la dogmática española hasta fecha relativamente reciente que puede fijarse en la mitad del siglo pasado. Esto no es del todo extraño, pues solo por aquella época empieza a reconocerse el derecho a la intimidad como objeto de protección penal diferenciado, además de que es entonces cuando empiezan a aparecer medios cada vez más insidiosos para atentar de modo impune contra este bien jurídico³⁵⁵. Ahora bien, siguiendo a ARROYO ZAPATERO encontramos que, debido al carácter fragmentario del derecho Penal, éste interviene únicamente en los casos más graves de atentados contra la intimidad. El resto, encuentra adecuada tutela en la vía civil o a través de los mecanismos administrativos previstos en la LOPD 15/1999³⁵⁶.

El Código Penal Español vigente, Ley Orgánica 10/1995, de 23 de noviembre, en cumplimiento de lo establecido por la constitución de 1978, protege mediante el Título X, delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, lo concerniente al descubrimiento y la revelación de secretos. Sin entrar al detalle, aun persisten críticas a la forma cómo está redactado este título, inclusive se le señala como atormentada e inacabable³⁵⁷ y de difícil concreción, en alusión a que sólo del art. 197.1, se

porque además en épocas anteriores no se producían las amenazas a la vida privada que actualmente existen y consecuentemente, la necesidad de preservar una esfera recoleta de la personalidad al cobijo del mundo exterior no era tan acuciante. Sobre lo anterior, estoy de acuerdo con el autor al señalar que el “impacto” que tienen las nuevas tecnologías ha redimensionado la afectación a este derecho, pero no creo que anteriormente, con las limitaciones de la época, no existiese violación al derecho de la intimidad, a lo mejor, como no se constituía en un derecho fundamental y menos en una conducta impropia, era común pasar por alto su desconocimiento.

³⁵⁵ OLMO FERNANDEZ – DELGADO, Leopoldo, El descubrimiento y revelación de secretos documentales y de las telecomunicaciones, estudio del artículo 197.1 del Código Penal, Edit. Dykinson S.L., año 2009, p.17

³⁵⁶ ARROYO ZAPATERO, Luis (Et al), Comentarios al Código Penal, Edit. Iustel, Madrid, p. 472

³⁵⁷ MORALES PRATS, Fermín, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del Domicilio”, en QUINTERO OLIVARES, Gonzalo (Dir.), Comentarios a la Parte Especial del Derecho Penal, 5 edición, Edit. Aranzadi, 2008, Navarra, p. 408

pueden desprender más de 15 modalidades típicas³⁵⁸ distintas de comisión del delito, bien en la conducta típica, bien en el objeto material. Del mismo modo, en este título el legislador regula los delitos de descubrimiento y revelación de secretos de una forma realmente complicada, con algún artículo que podría llevar a una inseguridad jurídica. De otra parte, la gravedad de las penas que se establecen para casi todos los supuestos puede llevar en algún caso a violar “el principio de culpabilidad”, pues a la infracción cometida se le fija una pena desproporcionada³⁵⁹. Por lo menos, dice MORALES PRATS, el Código Penal español ha encuadrado correctamente en un solo título diversas figuras delictivas que se encontraban en el código anterior penal diseminadas, bien en el título genérico de los delitos contra la libertad y seguridad de las personas, o bien en otros ámbitos del código. Sin embargo, señala que, a su juicio, en el rótulo del Título X hubiera sido más correcto aludir de forma exclusiva y lacónica a “Delitos contra la intimidad”³⁶⁰.

En sí, el art. 197 y sus distintos apartados desarrollan las diversas formas en las que se puede cometer delito contra la intimidad, algunos más modernos que otros claro está, pues muchos tendrán la capacidad de tomar una carta del buzón de otro. En término general (por ser un acto físico que no requiere mayor esfuerzo), pero solo algunos pocos, tendrán la capacidad o la preparación para interceptar comunicaciones de tipo electrónica y evidentemente capturar mensajes que se ubican más que en un terreno material, en el llamado ciberespacio.

Siguiendo con el art. 197.1. este artículo protege la intimidad de una forma más amplia de lo que lo hacía el art. 497 del Código penal anterior. En esta redacción se dice que

³⁵⁸ OLMO FERNANDEZ – DELGADO, L, Op. cit., p. 69

³⁵⁹ SERRANO GÓMEZ, Alfonso y SERRANO MAÍLLO, Alfonso, Derecho penal – parte especial, Edit. Dykinson, Madrid, 2009, p. 276

³⁶⁰ MORALES PRATS, Fermín, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en QUINTERO OLIVARES, Gonzalo (Dir.), Comentarios a la parte especial del derecho penal, 8 edición, Edit. Aranzadi, 2009, Navarra, p. 404

“el que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses”. A primera lectura, se le puede señalar como finalista, pues se determina que las conductas que realiza el sujeto, llevarán como resultado último, descubrir los secretos o vulnerar la intimidad de otro. Esto condiciona, por imperativo de la ley, a que la actividad realizada tiene que buscar este objetivo para poder encuadrarse dentro del tipo penal. Para MAURACH, se le puede aplicar el calificativo de estructuralmente incongruente, pues la norma extiende el tipo subjetivo más allá del objetivo³⁶¹.

5. Resumen de ideas.

La intimidad sigue siendo un concepto difuso y tal característica ha influido en la manera de proteger al paciente de la invasión no consentida de terceros. Este derecho se encuentra presente, de forma permanente, durante el ejercicio de la medicina y de las profesiones sanitarias, tanto en la medicina institucionalizada como en la privada, pues el médico es el receptor principal de múltiples informaciones que aporta el enfermo para lograr su curación.

En este orden de ideas, el núcleo esencial del derecho a la intimidad supone la existencia y goce de una órbita reservada para cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural.

³⁶¹ MAURACH, Reinhart, Tratado de Derecho Penal, Edit. Ariel, Barcelona, 1962, p. 274

El derecho a la intimidad no es absoluto, por lo que puede ser objeto de limitaciones en su ejercicio, sin que por ello se entienda que pueda desconocerse su núcleo esencial. En este sentido, queda claro que tal derecho puede entrar en conflicto con otros de igual interés y prevalencia, como es la libertad de información o expresión, las que imponen limitaciones a la intimidad personal.

Ahora bien, el profesional sanitario para prestar una buena y adecuada asistencia, tiene que callar la información que conoce del paciente, pues es una relación basada en la confianza, lo cual resulta muchas veces difícil dada la realidad asistencial. De no cumplirse con estos criterios mínimos, difícilmente el paciente abrirá toda su realidad ante el médico y éste no podrá cumplir con su propósito, si desconoce todo el panorama que afecta al enfermo.

En cuanto a la confidencialidad, es también considerada como una actitud que se le pide al sujeto conocedor del dato o hecho de la intimidad o privacidad de la persona, lo que supone una obligación del profesional de mantener en secreto cualquier información proporcionada por el paciente, no pudiendo revelársela a un tercero sin su permiso específico. Dicho así, parece evidente en la investigación que la confidencialidad es un concepto próximo a la intimidad, de manera que cuanto más íntimo sea el dato, será preciso un mayor grado de confidencialidad.

En definitiva, es justo reafirmar que el derecho a la protección de datos personales es independiente y autónomo respecto al derecho a la intimidad y abarca una mayor amplitud de situaciones, pues protege datos personales sean íntimos o no, bastando que sean datos que identifiquen o permitan la identificación de una persona y, además, lo hace con independencia de si se encuentran almacenados por sistemas informáticos o de cualquier otra forma.

Aun así, el derecho a la protección de los datos y la intimidad, pueden ser ampliamente vulnerados en los historiales clínicos, lo que obliga al paciente a conocer qué derechos posee ante esta situación, cómo puede proteger sus datos y qué obligaciones tiene el personal sanitario por la entrega de su información personal.

De todo lo anterior, queda por conocer qué herramientas existen para proteger estos derechos, a qué se refiere la norma con los derechos ARCO y cómo puede el ciudadano ejecutarlos de ser necesario. Asimismo, la investigación se concentrará en adelante en conocer aspectos tan importantes como el secreto profesional y demás estrategias que plantea el derecho, en defensa del derecho que tiene el paciente a mantener en reserva su condición de salud.

Por ejemplo, el secreto profesional encuentra su fundamento en la Constitución Española (art. 18.1 y 20 CE) y también goza de regulación en los diferentes sectores del ordenamiento jurídico interno (administrativo, civil, laboral, procesal y penal), así como en el Derecho internacional y comunitario.

Sobre lo anterior, se continúa en el último capítulo de la investigación, con el análisis de los medios que tiene la persona para proteger sus datos de salud, elemento que encuentra justificación debido al constante cambio que existe en ellos y el interés de mantener tal información lo más clara y exacta posible.

CAPITULO 5

MEDIOS PARA PROTEGER LOS DATOS DE SALUD DEL PACIENTE

SUMARIO: 1. Aproximación al tema. 2. Los derechos de acceso, rectificación, cancelación y oposición. 2.1. El derecho de acceso. 2.1.1. El estado de necesidad terapéutica. 2.1.2. Otro tipo de accesos. 2.2. La rectificación. 2.3. La cancelación. 2.4. El derecho de oposición. 2.5. Los derechos ARCO y los herederos del paciente. 3. La obligación de callar los datos de salud. 3.1. ¿Es necesario el secreto médico? 3.2. Fundamento histórico del secreto profesional. 3.3. Criterios que le dan fundamento. 3.4. Bases legales para el secreto médico. 3.5. Límites al secreto médico. 3.6. Excepciones al secreto médico. 3.6.1. Consentimiento del paciente. 3.6.2. Autorización de la ley. 3.6.3. La declaración de enfermedades. 3.6.4. El registro de nacimientos y defunción. 3.6.5. Revelar el secreto a favor del paciente o de un tercero. 3.6.6. Revelación en favor del propio médico. 3.7. El secreto y el médico de la empresa. 3.8. El secreto y el médico forense. 3.9. Diferencias entre el secreto profesional del médico y el secreto profesional del abogado. 3.10. La revelación de secretos en el código penal español, artículo 199. 4. Resumen de ideas.

1. Aproximación al tema.

Hasta este punto la investigación ha planteado las diversas normativas vigentes, encargadas de proteger los datos personales, la historia clínicas y los derechos fundamentales que en ella existen, haciendo un énfasis en el derecho a la protección del dato de salud y el derecho fundamental a la intimidad.

En efecto, aunque la normativa existe y no hay discusión en la validez de sus enunciados, la vida diaria nos muestra que es usual la presentación de quejas, por parte de los ciudadanos, al ver que sus derechos han sido vulnerados en diversos casos.

Sobre el particular, si bien existen los derechos de acceso, rectificación, cancelación y oposición (ARCO), para defender a la personas, es la propia conducta del titular de los datos la que se constituye en la primera garantía para la protección sus derechos. De tal forma que, si se facilitan datos personales sin leer previamente la información sobre privacidad, si no aprende a configurar el perfil en una red social, o si expone abiertamente información personal en red, no es de extrañar que se exponga a riesgos innecesarios.

La creciente injerencia del Estado en los asuntos del particular genera mayores inquietudes, y se acumulan un mayor número de reclamaciones ante la Agencia de Protección de Datos, por la utilización incorrecta de datos personales en la esfera de ficheros de morosidad, la video vigilancia en distintas áreas y la utilización de red para saltarse las medidas de seguridad aplicable a los datos, con la consecuente difusión no autorizada de la información.

En razón de lo anterior, no puede olvidarse que la salud también es un bien social que abarca un campo de actuación más amplio que el meramente asistencial. Por ello, para aprobar el acceso a los datos sanitarios, primero debe considerarse con detalle el principio de proporcionalidad, entre el derecho a reservar la información del paciente y los intereses de las otras partes. En todo caso, por ejemplo, el historial médico puede contener información tan variada, que sería de especial interés para distintos sectores. Pero, ese interés no implica que se pueda utilizar sin control la información del enfermo, ni siquiera los médicos que tienen acceso directo a esta, pueden hablar de su contenido y detalles propios de la atención médica.

Por este motivo, en este capítulo se presenta una evaluación del deber de secreto, como primera obligación del médico a callar los datos de salud de su paciente y tal como se mencionó en capítulos anteriores, este tipo de secreto se asocia directamente a la

profesión por ser el médico y el personal sanitario quienes están obligados directamente con el deber de callar. Igualmente, la obligación de guardar secreto se extiende a todos los profesionales de la salud no solamente a los médicos, ya que todos ellos en el ejercicio de su profesión, tienen acceso a datos sanitarios del paciente.

2. Los derechos de acceso, rectificación, cancelación y oposición.

Con el fin de salvaguardar los intereses de las personas, y del paciente en especial, el derecho fundamental a la protección de datos, al igual que el derecho fundamental a la intimidad, permiten la negativa en la intromisión de la vida privada, y, además, obliga al responsable del fichero a mantener un control sobre la información que posee y responder ante las consultas y quejas que puedan generarse por su custodia y posterior utilización. Con este derecho, de configuración jurisprudencial³⁶², se asegura a su vez, que quien ostenta la información debe ser una persona conocida por el paciente, ante quien puede recurrir y de quien puede esperar respuesta en aquellos casos en los que considere que su información no es acorde con su situación actual. No obstante, esto no quita que tal uso de los datos de salud y la intromisión en la vida del paciente sea siempre negativa, ni que se pretenda un ataque a su entorno privado, pues “en el campo de la sanidad, no es posible ofrecer una asistencia adecuada sin conocer datos, hechos y actuaciones de la persona que ésta guarda para sí misma y que forman parte de su esfera íntima, de manera que el usuario ha de abrir necesariamente su intimidad para que la prestación se lleve a cabo eficazmente”³⁶³.

³⁶² PALOMAR OLMEDA, Alberto, “Confidencialidad y protección de datos en la Ley de salud sexual y reproductiva y de interrupción voluntaria del embarazo, cuatro estudios”, en Revista Derecho y Salud, Volumen 20, núm. 2, Julio – Diciembre, 2010, p. 69

³⁶³ GARCÍA AMEZ, Javier, “La protección de datos del usuario de la sanidad: derecho a la intimidad y asistencia sanitaria”, en Revista Derecho y Salud, Volumen 20, núm. 1.1, Enero – Junio, 2010, p. 45

En este sentido, durante los capítulos anteriores, se hizo referencia a la protección del secreto profesional y los medios penales que tiene el enfermo para proteger su historia clínica, sobre todo porque “este documento ha trascendido ampliamente su ámbito, e incluso el marco de la estricta relación médico – paciente, extendiéndose a otros contextos como los seguros, la seguridad social y las relaciones laborales”³⁶⁴. Ahora debemos destacar que, en cuanto a la protección de datos, la persona cuenta con elementos esenciales, tales como la información y el consentimiento, como métodos previos de protección, dado que ambos impiden que se interfiera a la ligera, con la normalidad de su vida. Sin embargo, ¿qué sucede cuando la información ya ha sido obtenida por otra persona y el derecho a controlar los datos personales se ha visto afectado? En estos casos, existen otras opciones jurídicas para restablecer dicho control y la LOPD 15/1999, no es silente este aspecto, ya que atribuye al afectado “un conjunto de mecanismos reactivos que constituyen una parte del contenido esencial del derecho fundamental a la protección de datos. Estos mecanismos se concretan en los derechos de acceso, rectificación, cancelación y oposición regulados en los artículos 15 y siguientes de la ley”³⁶⁵.

Efectivamente, estos derechos se basan en la facultad que tiene el individuo de pedir información y así conocer qué datos de salud poseen de si mismo, cómo los han obtenido, para qué se están utilizando y quiénes han tenido acceso a ellos. En esta materia DAVARA RODRÍGUEZ deja claro que el “derecho de pedir información”, puede ser confundido con la “obligación de informar”, porque en la práctica es mediante este derecho cómo el afectado obtiene, o debe obtener, una información exacta y veraz sobre sus datos de carácter personal que se encuentran en el fichero o, en su caso, información sobre que el

³⁶⁴ HEREDERO HIGUERAS, Manuel, La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal, Op. Cit., p.108

³⁶⁵ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0593-2009, p. 3

fichero no contiene ningún dato de carácter personal sobre él mismo³⁶⁶. Además, siguiendo a ALVAREZ GONZÁLEZ, dice que “el derecho de información adquiere una especial relevancia en el ámbito sanitario, ya que a través de la transmisión de los datos de salud al sujeto, éste podrá conocer qué tipo de información se ha obtenido de las diferentes pruebas y exploraciones, con qué finalidad, quién tiene conocimiento de la misma y en dónde queda registrada”³⁶⁷.

Estos derechos, también conocidos como derechos ARCO, buscan principalmente apoyar al individuo, en nuestro caso el paciente, para re establecer la confidencialidad de su información, pese a que la misma se encuentre en un fichero automatizado o no, o en poder de terceros no autorizados. Las nuevas tecnologías han probado que estos mecanismos de control previo a la obtención de la información no son los más efectivos en todos los casos, y no sorprende que existan ficheros muy completos sobre el estado de salud de una persona, sin que ésta siquiera sospeche de su existencia. Además, las herramientas de informática actuales “permiten que se superen las barreras espaciales y temporales que la realidad física impone y posibilitan que el tratamiento de la información, y en concreto su transmisión, se realice de forma más rápida y de manera internacional”³⁶⁸. El peligro está a su vez en el anonimato³⁶⁹ que se facilita en la red, lo que ha disparado las alarmas de todos los usuarios

³⁶⁶ DAVARA RODRÍGUEZ, Miguel A., Guía práctica de protección de datos, desde la óptica del titular del fichero, Universidad Pontificia de Comillas, 1999, p.66

³⁶⁷ ALVAREZ GONZÁLEZ, Susana, “El habeas data biosanitarios: especiales situaciones de conflicto en relación con los datos genéticos, en GARRIGA DOMINGUEZ, Ana y ÁLVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos personales, especial referencia al registro obligatorio de los portadores del VIH, Op. Cit, p.60

³⁶⁸ ABERASTURI GORRIÑO, Unai, “Movimiento internacional de datos. Especial referencia a la transferencia internacional de datos sanitarios”, en Revista de Administración Pública, núm. 186, Septiembre – Diciembre, 2011, p.330

³⁶⁹ Y es que el anonimato trae como consecuencia que cualquiera persona puede conocer ilegalmente una información, bien sea para sacar un provecho económico o simplemente para fastidiar al prójimo. Lo cierto es que las redes sociales, como Twitter o Facebook, han redimensionado el impacto que tiene la tecnología en la

de los servicios de atención médica, y ahora es más fácil conocer la verdadera condición de salud de una persona, pues basta con un sistema desprotegido o logrado clandestinamente, para que se expongan ante la opinión pública los datos de salud que tanto se pide reservar, o en su defecto “se pierdan, se alteren, o sean aprendidos por sujetos que quieran emplearlos de manera contraria a derecho”³⁷⁰.

2.1. El derecho de acceso.

El derecho de acceso que asiste al paciente, para conocer los datos de salud que poseen de él, se basa en distintos cuerpos legales, que van desde la Carta de los Derechos Fundamentales de la Unión Europea, que en su artículo 8.2 reconoce que "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación"; pasando por la Directiva 95/46/CE, del PE y el CUE que señala en su artículo 12 el derecho de acceso y sus características hasta llegar al nivel estatal, específicamente en el texto del artículo 15 de la LOPD 15/1999, se señala que “El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos”; y en el texto de la LOAP 41/2002, que en su artículo 4.1 establece el derecho que tienen “los pacientes 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”.

protección de los datos y en especial en los datos de salud. Gracias a los ordenadores y a la red de Internet, ahora la comunicación es mucho más simple pero de impacto mundial, haciendo que el envío y difusión de los datos de salud de una persona no esté limitado ni al tiempo ni a las fronteras físicas.

³⁷⁰ ABERASTURI GORRIÑO, Unai, “Movimiento internacional de datos. Especial referencia a la transferencia internacional de datos sanitarios”, Op. Cit., p.331

El derecho de acceso, también conocido como derecho de habeas data³⁷¹, está muy vinculado con el principio de transparencia y permite a las personas³⁷² físicas, en nuestro caso los pacientes, conocer la información que se tiene sobre sus datos de salud, de forma gratuita y expedita, para después valorar la calidad de la misma y decidir en cuanto a su permanencia o no en un fichero determinado, respetando evidentemente las restricciones impuestas por la LOAP 41/2002. Estos derechos no son reconocidos a las personas jurídicas, y menos para el tema de salud, ya que por su propia naturaleza de creación, las personas jurídicas son una “ficción jurídica” y no nacen por vía natural, sino por disposición de la ley, lo cual les impediría que pudiesen contar con cuerpo y salud física, merecedora de protección por parte de la legislación actual. Asimismo, tal como señala HERRAN ORTIZ, “no puede por menos reconocerse el acierto de la definición que identifica al sujeto activo del derecho a la autodeterminación informativa con la persona física que ostenta la titularidad de los datos personales que son objeto de tratamiento automatizado. En otras palabras, se reconoce la condición de sujeto activo del citado derecho a las personas a quienes afecta o se refiere la

³⁷¹ Bien pudiera decirse que este es un derecho, constitucional o legal, según sea el caso, que tiene cualquier persona, de acceder a los registros y ficheros que tenga otra persona, natural o jurídica, pública o privada, para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio.

³⁷² Se entiende dentro de este concepto, a todas las personas físicas, sin distinción de nacionalidades o su estatus jurídico. Análisis reiterado por HERRÁN ORTÍZ, Ana, La violación de la intimidad en la protección de los datos personales, Dykinson, 1999, pp. 233 y 234. La autora también deja notar el “desliz” cometido por el artículo 18.4 de la Constitución cuando señala que “la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. No sólo incomprensible, sino además injustificada, resulta la limitación constitucional en la condición de sujeto activo del derecho de autodeterminación informativa. Coincidimos totalmente con ella, pues no se explica cómo si el artículo 18 reconoce el derecho a la intimidad de manera general todas las personas, qué motivó al legislador constitucional a limitar la titularidad del derecho a la autodeterminación informativa y restringirla a los ciudadanos.

información que les identifica como tales, y que se almacena, registra, cede, modifica o cancela”³⁷³.

En vista que los datos se recogen en principio con el consentimiento previo de la paciente, algunos autores³⁷⁴ sostienen que es lógico que éste conozca la existencia del fichero y simplemente quede a su consideración la decisión de verificar cuanta información se acumula sobre él. Asimismo, ponen de manifiesto que es precisamente esta “acumulación de datos” la que puede arrojar un perfil de las personas y después poner en riesgo su derecho a mantener en reserva su información. Sobre este aspecto, yo creo que, en términos generales es así, y lo normal sería que el paciente “presuma” la existencia del fichero después de ser atendido en un centro hospitalario. Por ejemplo, pero no debemos olvidar que no todos los datos de salud se encierran en una historia clínica y también pueden estar dispersos en múltiples ficheros, sin vinculación a un tratamiento sanitario.

Pero que difícil resultará para el interesado saber cuál información pedir, por ser muy amplia la cantidad de datos que se acumulan para el tratamiento del paciente. Cabe señalar que algún problema produce la no delimitación de cuánta información de salud debe recabarse por cada usuario para después considerarse completa, lo que algún sector suele llamar la longitud del dato, de ahí que se puede obtener mucha o poca, dependiendo de la habilidad de quién pregunte o de los propios protocolos de atención. Y es que, tal como hemos mencionado en el Capítulo dedicado a la historia clínica, la anamnesis o etapa de entrevista entre el médico y el enfermo sería el momento cuando se recogen las informaciones generales sobre el estado del paciente antes de ser ingresado para

³⁷³ HERRÁN ORTÍZ, Ana, La violación de la intimidad en la protección de los datos personales, Dykinson, 1999, p. 236

³⁷⁴ Cf. APARICIO SALOM, Javier, Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Aranzadi, 2002, p.153. Idem, VÍZCAINO CALDERÓN, Miguel, Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas, 2001,p.195

tratamiento médico, y después durante su estancia se irán sumando los otros datos que surgen producto del diagnóstico y tratamiento según cada caso, pero no está definido cuánto se debe preguntar para llegar a un buen diagnóstico, o cuántos datos de salud propios y de familiares debe revelar el enfermo, para guiar a su médico en la búsqueda de su cura. De igual forma, dado que la atención curativa es en equipo, cada especialista puede recabar su propia información, acorde a sus propias necesidades de investigación y bajo múltiples medios o pruebas clínicas, siendo muy extensa la cantidad de datos que se irán acumulando en el historial clínico que, como veremos, puede estar ubicado en diferentes partes, según el nivel de afectación que tenga el enfermo en su salud.

Más interesante aún, resulta el análisis que hace GARCÍA AMEZ sobre los “hallazgos inesperados”³⁷⁵, los cuales define como aquella información novedosa, desconocida por el paciente, que surge después del tratamiento de sus datos, y que fue visible gracias al uso de la información que el enfermo aportó inicialmente a su médico. Según comenta el autor, en estos casos surge otra obligación para el responsable del fichero, la de comunicar esta novedosa información a su titular, para así justificar su tenencia, previo al tratamiento del dato. Esta afirmación la entendemos en los casos de pacientes que, producto de unas pruebas analíticas para tratar una cardiopatía, por ejemplo, le identifican además que padece otra enfermedad, y se requiere incorporar su información dentro del fichero correspondiente a los pacientes con esta patología. En consecuencia, siguiendo al autor, no es permitido al responsable del fichero tratar “de facto” este nuevo dato de salud, sin informar previamente al paciente sobre su existencia y lograr de éste su aprobación, como requisito previo a proceder con su uso. En cuanto a lo anterior, debo decir también que informar al paciente sobre toda su condición de salud, puede igualmente tener efectos adversos, sobre todo si se toma en cuenta el estado de necesidad terapéutica que comentaremos más adelante.

³⁷⁵ GARCÍA AMEZ, Javier, “La protección de datos del usuario de la sanidad: derecho a la intimidad y asistencia sanitaria”, en Revista Derecho y Salud, Volumen 20, Op. Cit., p. 63

En cuanto al método de acceso a la información, la misma LOPD 15/1999 señala que una alternativa viable será la simple visualización, lo que a mi criterio ya representa una ventaja para el paciente, puesto que lo libera de costos o tasas que pagar por la emisión de documentos o copias, pudiendo conocerla sin mayor inversión de recursos económicos, que en ocasiones son muy limitados. De igual forma, deja abierta la opción para aquellos casos en los que la información pueda entregarse por escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. Las múltiples opciones, a su vez, son más que pertinentes a mi criterio, si tomamos en cuenta a las nuevas tecnologías que acompañan al servicio de salud. Ahora existen los correos electrónicos, que pueden ser consultados desde dispositivos fijos y hasta móviles, lo que representa una forma expedita de recibir información. El hospital puede sugerir algunos métodos que considere prudentes, para lograr el acceso por parte del paciente, medios que deben certificar que son expeditos y seguros pero, sobre todo, que puedan garantizar economía para el usuario. No obstante, aun así el paciente tendrá derecho a elegir uno distinto, que a su parecer cuente con mayores ventajas.

Por contra, si el medio que pone a disposición el responsable del fichero cumple con todas las condiciones, pero es rechazado por el usuario, deberá éste asumir los costos adicionales que implique la utilización del medio seleccionado por éste. Sin embargo, hay que aclarar que cualquiera que sea el medio elegido por el paciente, será él el responsable de la seguridad de los datos que se entreguen. Pensemos que se elige una cuenta de correo electrónico, pero que el mismo paciente no controla completamente sus claves de acceso. En este sentido, si el hospital cumple con la obligación de enviar los datos por este medio, y los mismos son conocidos por terceros, sólo el paciente sería responsable por la liberación de la información.

Igualmente, son de vital importancia las siguientes previsiones mencionadas en la LOPD 15/1999 y su reglamento el Real Decreto 1720/ 2007, en especial las que se refieren a la no utilización de códigos o claves dentro de la información entregada, ya que, de hacerlo, automáticamente dejaría en indefensión al paciente, por no entender lo que allí se describe, peor si para hacerlo necesita de otros recursos con los que no cuenta, lo que supondría una limitación ilegal a su derecho. En igual sentido, es importante la obligación de no utilizar un lenguaje complejo, puesto que tal comportamiento dejaría vacío de contenido a la protección legal que pretende el artículo. Sobre esto último, sí aceptamos que es un reto para la entidad sanitaria, adecuar el lenguaje técnico de los diagnósticos y pronósticos del paciente al vocabulario cotidiano del paciente, a lo mejor los datos personales no implican mayor dificultad, pero un cuadro complejo por naturaleza, como una cardiopatía, por ejemplo, a veces tiene un grado de dificultad para expresarse en términos más coloquiales o compatibles con una lectura sencilla.

Del mismo modo, también hay que decir que el derecho a tener acceso a la información de salud no es absoluto, ni está por encima de los derechos de otras personas, mucho menos se puede ejecutar de forma arbitraria y sin control. El Real Decreto 1720/2007, en su artículo 30, fija los periodos de consulta en 12 meses, salvo justificación para realizarse antes. En estos casos, se permite al responsable del fichero negar el acceso a la información, cuando se concurren dos supuestos: que la información se pida en intervalos de tiempo menor a 12 meses y que no medie justificación para dicha solicitud, o que el derecho lo ejercite una persona distinta al paciente.

En si, deben existir razones válidas para que se reduzca este periodo prudencial de doce meses. Pero, para lograrlo, surge la obligación para el interesado de motivar la solicitud, la cual será considerada y evaluada. Y, de existir motivos suficientes, entonces se permitiría el acceso de la información en plazos menores a los establecidos por la ley. En todo caso, dice VIZCAÍNO CALDERÓN, “el sentido de la norma es perfectamente lógico y

responde tanto a la seriedad con la que se configura el derecho de acceso, cuanto a la necesidad de evitar que el responsable del fichero se vea acosado por reiteración de peticiones superficiales, caprichosas o no debidamente justificadas³⁷⁶. Aun así, aunque comprendo perfectamente el ánimo del legislador de evitar un desgaste innecesario al responsable de fichero, producto del uso excesivo del derecho por parte del paciente, me queda alguna preocupación por el término de doce meses, dada la actualidad en la que vivimos, en los que la información apoyada con los recursos tecnológicos no está sujeta a territorios ni fronteras, y lo que en este instante sucede en un extremo del plantea, puede ser conocido casi al instante en el otro extremo. Me hace pensar si los periodos anuales no merecen ser revisados. El cambio en la información de salud es una constante que a lo mejor no está sujeto a periodos amplios como lo es doce meses.

A todo esto, tampoco queda tan claro cuál es la cantidad de información que se debe mostrar y, por tanto, algunos responsables de ficheros se muestran renuentes a exponer todo lo que poseen de un particular y ni siquiera le es fácil entregarla para propósitos judiciales, por lo que "hay que tener en cuenta que cualquiera que sea la extensión que se reconozca al derecho de acceso previsto en el artículo 15 de la ley orgánica de tanta cita, no puede tener, si nos atenemos a criterios de proporcionalidad..., una eficacia obstructiva, impeditiva o limitadora de la tutela judicial efectiva que dispensan jueces y tribunales cuando se formaliza una contienda judicial"³⁷⁷. Sobre esto, para un caso en particular, la Audiencia Nacional aclara que "los datos que deben proporcionarse por el cauce del derecho de acceso, son todos aquellos datos relativos a la determinación y constatación de sus lesiones, su evolución y, en su caso, las secuelas advertidas, que afectan a la salud de la titular de los datos, pero no pueden incluirse, como " datos de base", las valoraciones o

³⁷⁶ VIZCAÍNO CALDERÓN, Miguel, Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas, 2001, p.196

³⁷⁷ SAN, de 30 mayo de 2007, FJ: 5 (RJCA 2007\448)

apreciaciones de índole médica sobre el encaje de las lesiones o secuelas padecidas en la aplicación del baremo del Real Decreto Legislativo 8/2004”³⁷⁸.

En ese sentido, este derecho estaba reglamentado por la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación y; más adelante, se desarrolló también por el Real Decreto 1720/2007 el cual establece en su artículo 27.1 que “el derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos”.

Antes de continuar, conviene analizar un poco la estructura de este artículo 27.1 y destacar que el derecho de acceso corresponde al afectado. Debemos entender que no se espera que una persona distinta trate de ejercerlo, salvo las excepciones antes mencionadas. Lo que busca este derecho es ingresar a la información, pero no cualquiera, sino la del paciente en particular. No puede entonces, con base en este derecho, tener acceso a información de otros enfermos, ni de los profesionales que lo atienden y lo hace con el ánimo de conocer si su información está siendo objeto de tratamiento.

En si, estos derechos son y deben ser ejercitados por el afectado solamente, entendiendo con esto a la persona dueña de información de salud, salvo los casos especiales por representación, como son las personas con discapacidad y los menores de edad o en los casos cuando el propio paciente consienta que familiares y demás accedan a ella, al igual que aquellos casos en los que el paciente por sus propias condiciones de salud, no pueda otorgar el consentimiento, entre otros. De esto, también hay que aclarar que, aunque la actuación

³⁷⁸ SAN, de 30 mayo de 2007, FJ: 6 (RJCA 2007\448)

ante el responsable del fichero puede hacerse mediante apoderado o representante, la decisión sobre si se ejercita el derecho o no, nunca podrá cederse a persona distinta al interesado, pues la ley sólo este derecho como personalísimo.

En este sentido, se deja sentado mediante Informe Jurídico de 1999 de la Agencia de Protección de Datos que, “no son admisibles los apoderamientos genéricos, sino aquéllos que se refieran concretamente al ejercicio de alguno de los derechos consagrados por la LOPD 15/1999 ante los responsables de los ficheros, indicando los términos en que el apoderamiento se realiza, sin que el mandatario pueda, en modo alguno, exceder de lo dispuesto en esos términos y sin que quepa atribuir al mismo una potestad genérica de actuación. Esta atribución genérica desvirtuaría la exigencia contenida en el artículo 11 del real Decreto 1332/1994, por cuanto no supondría una concreta manifestación de la voluntad del interesado de ejercitar los derechos, toda vez que éstos serían ejercidos únicamente si el apoderado lo considerase oportuno y en los términos en que el mismo estimase adecuados”³⁷⁹. Sobre este tema, tal mandato al representante debe contar con las formalidades propias para trámites legales³⁸⁰, ya que sería la forma más adecuada de hacer constar ante el responsable del fichero que quien toma la decisión es el interesado y no otra persona. El informe también destaca que, aunque el representante legal está facultado para

³⁷⁹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico de 1999, p. 2

³⁸⁰ El Informe Jurídico de 1999 aclara que para estos casos, se exige que el mandato no sea verbal, puesto que sólo mediante un apoderamiento escrito podrá conocer el responsable del fichero la concreta voluntad de ejercicio del derecho por el afectado y, si el apoderamiento fuera efectuado mediante documento privado sería preciso, a fin de que el mismo pudiera dar fe ante el responsable del fichero, que dicho apoderamiento deriva directa e inequívocamente del interesado, titular del derecho protegido, que la firma de éste último apareciera autenticada mediante medio que permitiese a aquél tener perfecto conocimiento de que la declaración de voluntad procede inequívocamente del propio afectado, aportándose por el representante el original de dicho apoderamiento. Por último, será posible el ejercicio del derecho por apoderado cuyo poder aparezca otorgado en escritura pública, siempre y cuando dicho apoderamiento cumpla los requisitos de contenido a los que nos hemos referido con anterioridad.

reemplazar en “los trámites” al paciente, eso no significa que dicha representación le permita abrogarse una decisión tan esencial como la de “activar” sus derechos, en todo caso, el paciente es libre de decidir si quiere o no, acceder, rectificar o cancelar la información que existe en los ficheros y, por el contrario, puede asumir una actitud permisible, si esto le resulta adecuado a su parecer.

Entre las garantías que establece el Derecho está la obligación del responsable del tratamiento de explicar al interesado cuál ha sido la finalidad de esta recolección de sus datos, en caso de que no lo hubiese explicado inicialmente, justificar cómo los obtuvo e informar si estos datos se han compartido con otras personas, bien sea un encargado del tratamiento o una cesión de datos directamente. En ambos casos deberá probar si cuenta con el consentimiento para este tipo de acto. En si, deberá comunicar quiénes han recibido los datos del paciente, por ejemplo, antes de que éste haya presentado su solicitud de acceso y quiénes podrían recibirlos posteriormente. Esto implica que el responsable del fichero, tendría que mostrar mediante pruebas, con quiénes ha tenido relación en el uso de los datos del paciente, bien sea mediante acceso en su propia organización o cesión de los mismos ante terceros.

No es obligatorio, ni la ley manda, que la información, después de ser pedida, se entregue totalmente, el paciente puede decidir sobre qué información le interesa con mayor fuerza o bien puede pedirla de manera íntegra y el responsable del fichero deberá entregarla en los términos solicitados, salvo casos excepcionales, como el estado de necesidad terapéutica, que abordaremos posteriormente. De esto, el responsable de fichero, para casos de mucha complejidad como dice la norma, podría pedir al paciente un detalle de los aspectos que le interesa conocer, para dar respuesta de forma más eficiente al derecho de acceso. Pensemos, por ejemplo, en una persona que quiere saber sobre los datos correspondientes a una cirugía que le ha sido practicada, pero sólo en cuanto a los resultados de la misma, y no al cúmulo de pruebas analíticas realizadas previamente a la misma.

Sobre lo anterior, podría interpretarse la obligación “expresa” que establece el Real Decreto 1720/2007, en su artículo 32.2. al tiempo que tome en responder, pero no a su contenido, pues igualmente una entidad puede responder en tiempo record ante una solicitud, pero no necesariamente entregar todos los datos que posee del paciente. En este aparte nos parece que hubiese sido mejor que el artículo incluyera, además, del “tiempo de la respuesta”, una referencia al contenido, sobre ¿cuánto se puede pedir? ya que por más que establezca que “dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos”. Pensemos, por ejemplo, en los casos de un paciente, que para presentar una reclamación judicial o para estudiar si existe la posibilidad de una acción legal contra un médico o un centro sanitario, por un tratamiento que considere incorrecto, solicite el acceso a múltiple información de su historia clínica. De poco o nada servirá que la misma le llegue rápido, pero a cuenta gotas, si mediante el fraccionamiento de la información se puede diluir su derecho. VIZCAÍNO CALDERÓN señala en este aspecto “que el objetivo del derecho se concibe en términos muy amplios. No parece que exista restricción objetiva en punto al contenido de la información. Todo lo que afecta a sus datos de carácter personal almacenados en el fichero, le deberá ser informado si así lo pide”³⁸¹.

Sobre el alcance de la información pedida, y si corresponde entregarse en su totalidad, se ha pronunciado el Tribunal Supremo al señalar que este tema no ha sido resuelto aun por la normativa actual, ni siquiera por la reglamentación de la LOPD 15/1999, ya que “la indefinición también se observa en el Real Decreto 1720/2007. El artículo 27.1, al definir el derecho de acceso como “el derecho del afectado a obtener información sobre si

³⁸¹ VIZCAÍNO CALDERÓN, Miguel, Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, Op. Cit., p.193

sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dicho datos y las comunicaciones realizadas o previstas de los mismos" , no concreta la extensión de la información, y esa falta de concreción no se supera en el apartado 2 cuando prevé que "en virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento"³⁸², pues esa mención a la totalidad de los datos, latente en la normativa analizada, habilita para afirmar que la información debe comprender todos los datos, pero no que todas las circunstancias que configuran los datos deban ser facilitadas.

La solicitud de acceso a la información debe dirigirse al responsable de fichero, por ser éste quien determina, según la ley, los fines y usos de los datos de salud, dentro de lo cual tiene un plazo de un mes para dar respuesta "expresa" ante la solicitud de acceso. Es importante destacar que el paciente debe utilizar un medio que permita acreditar el envío y recibo de la solicitud, para lo cual se empezará a contar el periodo de un mes, a partir de la fecha de recepción de la solicitud. No obstante, "este requisito no puede entenderse como una formalidad esencial para la validez del ejercicio del derecho, sino sólo para poder acreditar, en caso de ser preciso, cuando se solicita la tutela de los derechos ante la Agencia

³⁸² STS, de 11 marzo 2011, FJ: 4 (RJ 2011\2065) En esta sentencia, la Sala concluye que las valoraciones o apreciaciones de índole médico sobre el encaje de las lesiones o secuelas padecidas por la paciente, en el baremo del Real Decreto Legislativo 8/2004, no deben considerarse como "datos base" y sin que frente a tal valoración jurídica aduzca el Abogado del Estado razones que lleven a dicho Tribunal de casación a adoptar una solución distinta. Asimismo, con o sin una disposición reglamentaria como la del artículo 13.2 del Reglamento aprobado por Real Decreto 1332/1994, y por muy amplios que sean los criterios a la hora de determinar el contenido del derecho de acceso , sin duda esencial en la materia, la información, no puede extenderse a una circunstancia absolutamente secundaria y técnica cual es la ubicación de los datos sobre la salud facilitados en unos apartados de un baremo previsto con finalidad exclusivamente indemnizatoria.

de Protección de Datos, que efectivamente se ha realizado la solicitud”³⁸³. En este sentido, estamos de acuerdo con el autor sobre la imposibilidad del responsable del fichero a negarse a entregar la información, aduciendo que no se utilizó un medio que acredite la recepción de la solicitud. Consideramos en este caso que la constancia de recibo es una garantía más para el paciente, que refuerza su derecho a conocer sobre sus datos. Esta garantía sustentará con claridad las fechas o momentos desde cuándo se ejercitó el derecho y no puede, en todo caso, tener un efecto negativo sobre el afectado.

De igual forma, se puede pedir información y en este aspecto, el Informe Jurídico 0167/2005 de la Agencia de Protección de Datos ha señalado que “el derecho concedido al interesado por la ley únicamente abarcaría el conocimiento de la información sometida a tratamiento, pero no qué personas, dentro del ámbito de organización del responsable del fichero han podido tener acceso a dicha información, tal y como ha indicado ya esta Agencia de Protección de Datos al resolver cuestiones similares a la planteada en el presente supuesto”³⁸⁴.

Como ya hemos dicho, la voluntad del paciente determina quiénes acceden a sus datos de salud. Para el caso de los pacientes que han fallecido, también se tomará como base la voluntad, de modo que para aquellos casos en los que el enfermo haya prohibido que se revele su información, no podrán los familiares conocer o ejercitar el derecho de acceso a su información de salud. Esta condición puede tener excepciones, como corresponde a los casos en los que, “por riesgo de salud”, un familiar pueda justificar acceder a ciertos datos de salud del fallecido, previas motivadas razones. Un ejemplo común en estos casos son las enfermedades contagiosas y que pueden poner en peligro a familiares, o aquellas que por

³⁸³ Cfr. APARICIO SALOM, Javier, Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Op. Cit., p.156

³⁸⁴ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico, 0167-2005, p. 1

predisposición genética pudiesen influir en la calidad de vida o salud del familiar sobreviviente.

Debo decir que, en ocasiones, este derecho de acceso puede ser negado por seguridad de la propia comunidad o seguridad del Estado, para el caso de epidemias o enfermedades que puedan poner en riesgo la estabilidad de la ciudadanía en general, si la ley lo permite, este derecho de acceso puede verse limitado en su total cumplimiento, y sólo entregar la información que se considere básica, no siendo posible acceder a toda la que compila el Estado en este tipo de casos, aunque sea solicitada por el paciente. Aquí pueden tomarse como referencia los casos de las epidemias recientemente conocidas, como el H1N1, que planteó medidas especiales para contener la propagación del virus ante toda la población, en especial por los datos de viajeros y sus condiciones de salud, antes de ingresar o salir del país.

En caso de que no se pueda cumplir con la solicitud de acceso, es el responsable del fichero quien tiene que advertir al paciente, qué recursos caben, y ante quién puede ejercitarlos, en caso que se sienta inconforme con la negación a su petición.

Excepcionalmente, aunque hemos desarrollado casos en los que procede este derecho, destacamos que no todo acceso a los datos de salud, puede ampararse como es usual en los derechos reconocidos al paciente, por la LOAP 41/2002, ya que es imprescindible probar primero en estos casos la existencia de una relación entre médico y paciente, para después exigir el acceso total a la historia clínica. Pensemos en los casos de reconocimientos de daños o exploraciones de salud, pedidos por aseguradoras a sus equipos de médicos, previo a hacer efectivo el pago de una póliza, por más que exista un trato entre estos médicos y el cliente, no estaríamos frente a una relación asistencial o curativa. En este sentido, el informe médico realizado sobre las lesiones y secuelas del afectado no se enmarcaría en las relaciones tradicionales entre el médico y paciente, pues el objeto de la

exploración médica realizado no tendría por finalidad establecer un diagnóstico y prescribir un tratamiento para sanar o mejorar la dolencia, padecimiento o enfermedad, que constituye la esencia de la labor asistencial. Su finalidad es simplemente evaluar las lesiones y secuelas por encargo de la aseguradora, para determinar la cuantía del pago a realizar, por lo que la documentación de la exploración nada tiene que ver con la labor médica, tendente a curar la enfermedad de la persona, y por ende, tampoco tendría dicho propósito las historias clínicas que se elaborarían en estos casos. Sobre este tema, la Audiencia Nacional ha dicho que “no puede equipararse en modo alguno las historias clínicas que reflejan la imprescindible y específica relación entre el que padece una enfermedad y el profesional médico encargado de adoptar las medidas precisas para su curación o mejora, con el soporte documental de un informe encargado por un tercero (una aseguradora), a un médico para que evalúe la situación de una lesionada que, a su vez es o ha sido paciente de otro profesional de la medicina³⁸⁵”.

2.1.1. El estado de necesidad terapéutica.

Durante todo el desarrollo del trabajo hemos mencionado la gran importancia de dar información al paciente sobre sus datos de salud, el derecho que le reconoce la LOPD 15/1999 y el Real Decreto 1720/2007, para poder utilizarlos y la facultad que tiene para prohibir su cesión o comunicación a terceros. Sobre la propia información, debemos reiterar que los historiales clínicos no son la única fuente de datos de salud, “ni todo dato de salud es siempre médico, porque no siempre se utiliza en un contexto relacionado con la medicina”³⁸⁶, sobre todo cuando existen ficheros con este tipo de información en diferentes espacios, como son entidades de seguros, empresas farmacéuticas y otros, sin que estén condicionados a los parámetros de un hospital o centro sanitario, pero dado que “la

³⁸⁵ SAN, de 30 mayo 2007, FJ: 7 (RJCA 2007\448)

³⁸⁶ NICOLÁS, Pilar, “El Concepto de dato médico y genético”, en RIPOL CARULLA, Santiago (ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Marcial Pons, 2006, p. 79

manipulación de datos de salud se produce principalmente en el ámbito sanitario³⁸⁷ y que “la historia clínica es probablemente el documento que concentra mayor número de datos de carácter personal referidos a la salud y a la intimidad de la persona”³⁸⁸, me basaré en el análisis de los datos expuestos en estos documentos, haciendo énfasis en la diferencia que puede existir en cuanto al tipo de información que se vincula con la relación médico – enfermo y aquella en la que se pueden hacer excepciones de acceso.

La información que generalmente se logra en estos casos podría ubicarse en las siguientes características: información de tipo clínica, asistencial y terapéutica, dentro de la cual la primera corresponde a los datos recogidos por el médico durante la entrevista, aquí se incluyen las preguntas sobre la condición actual del paciente, padecimientos previos propios y de sus familiares: la segunda el que ofrece el médico, después de analizar las condiciones del paciente y así permitirle que pueda tomar la decisión clínica más acorde con sus intereses, de acuerdo a la naturaleza de su patología y las opciones diagnósticas, para esto, el médico debe incorporar sus conocimientos en el área de la medicina con las condiciones que presenta en enfermo, además, del conocimiento de la enfermedad, explicar las diversas posibilidades de tratamiento, evolución y pronóstico, según la elección que haga el paciente en cada supuesto.

Y vamos al centro de la cuestión, es en este último tipo de información en la que se podría, bajo supuestos muy especiales y amparados en la ley, negar acceso a la información de salud al enfermo, ya que en ocasiones, esta condición es tan compleja que podría afectar negativamente su recuperación. Esta excepción subyacente en los objetivos de

³⁸⁷ ABERASTURI GORRIÑO, Unai y LASAGABASTER HERRARTE, Iñaki, “La cesión de datos de salud fuera del ámbito sanitario. Análisis de supuestos concretos en que la información sanitaria se transmite para el cumplimiento de fines distintos al de la protección de la salud de las personas”, en Revista Vasca de Administración Pública, Op. cit., p. 19

³⁸⁸ CASTELLANO ARROYO, María, “Problemática de la historia clínica”, en Información y Documentación Clínica, Madrid, Op. Cit., Vol. I, p.77

la propia ley. En este caso hablamos de lo dispuesto por el artículo 5, apartado 4 de la LOAP 41/2002, cuando señala que:

“El derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave. Llegado este caso, el médico dejará constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho”.

Esta facultad extraordinaria del médico³⁸⁹, conocida también como Privilegio Terapéutico, en el mundo anglosajón o Principio de Asistencia, en el Derecho Alemán, busca evitar más dolor psíquico y espiritual a un paciente, que ya se encuentra muy afectado por su situación de salud física, especialmente cuando el pronóstico es fatal o de graves consecuencias. Para LAPORTA “puede darse el caso de que la eficacia del tratamiento dependa de algún modo de la ignorancia por parte del paciente de algún extremo relativo a

³⁸⁹ Cfr. CASTELLANO ARROYO, María, “Problemática de la historia clínica”, en Información y Documentación Clínica, Volumen I, Consejo General del Poder Judicial, Ministerio de Sanidad y Consumo, 1997, p59. Esta autora señala que la información al paciente puede ser comunicada no solo por el médico, sino también por la enfermera, según su área de competencia, sin embargo al leer el contenido de la LOAP 41/2002 (art. 5.4), destacamos que la posibilidad de actuar sin informar al paciente se reserva exclusivamente al médico. Por tanto, es un permiso exclusivo para este tipo de profesional y no se aplica a todos los que participan en la atención del paciente. Sobre lo anterior explica que aunque la información puede proceder de estos dos profesionales, debe hacerse de manera integrada, para evitar confusiones en el enfermo y la pérdida de confianza en su tratamiento.

ese tratamiento”³⁹⁰. El autor se refiere en mayor medida a la autonomía del paciente para tomar una decisión y la obligación del médico de informar de manera “sencilla” los procedimientos técnicos que están a disposición del enfermo. Sostiene que hay un desbalance notable de la posesión de la información, en la que el médico la tiene toda y el paciente, generalmente, lo ignora todo. En este sentido, se analiza si para consentir basta con entregar una parte de la información solamente, o por el contrario debe poner en conocimiento del enfermo toda la información disponible, aunque eso implique la difícil tarea de determinar cuándo el paciente está “suficientemente” informado sobre las opciones médicas que posee.

Contrario a lo anterior, en términos del respeto al derecho del paciente, la información veraz puede tener incluso un valor terapéutico, pues permite al enfermo tomar sus propias decisiones y de ese modo asumir un control de su vida; también reiteran que con la verdad directa se evita la ansiedad que producen la incertidumbre y el engaño de su médico. Del mismo modo, los partidarios del acceso total a los datos de salud reiteran que reforzar el derecho del enfermo a la verdad no significa que toda información deba ser dicha de cualquier modo y en cualquier momento, más bien, debe facilitarse haciendo un balance entre el profesionalismo del médico y la voluntad de mantener una empatía con el dolor del otro. Siguiendo estas condiciones, según ellos, se fortalece el respeto por la persona rescatando la humanización de la relación personal entre el profesional y el paciente. Incluso, un paciente informado sobre su verdadera condición de salud es mucho más consciente de los efectos de su enfermedad o de los cambios que padece, lo que lo hace mucho más decidido a mejorar su condición clínica, suele seguir mejor con el tratamiento indicado y acostumbra a colaborar más con los especialistas que llevan su recuperación.

³⁹⁰ LAPORTA SANMIGUEL, Francisco J., “Algunas incógnitas del principio de autonomía personal en tratamientos médicos, en MENDOZA BUERGO, Blanca (editora), *Autonomía personal y decisiones médicas*, Thomson Civitas, 2010, p. 30

Sin embargo, en mi opinión, este tema no deja de ser muy complicado, pues la LOAP 41/2002, en su artículo 5.4. aunque define qué se entiende por “estado de necesidad terapéutica”, no aclara la forma de acreditar estos extremos. A veces las verdades directas no son la mejor opción, y todo dependerá del nivel de madurez con que asuma el paciente la enfermedad. Si dado el caso le resulta imposible detener o incluso frenar el avance de su condición, es lógico pensar que la calidad de la vida es más importante que su duración, y evitar que toda la información pueda afectar además el estado psicológico del paciente. A sensu contrario, si el interesado, siendo plenamente consciente de lo que hace y de las consecuencias de conocer su estado real, desea acceder a la información completa sobre su condición de salud, no debe imponerse este principio, ni tampoco negarle el acceso a los datos solicitados, haciendo obviamente las exclusiones previstas en la ley. Para esto hay que reconocer que cada persona es la más autorizada para juzgar y decidir sobre su propia realidad, aunque esto suponga más sufrimiento. Reiteramos que si el paciente conoce las consecuencias de su decisión, debe respetarse su derecho a conocer toda la información que le compete.

MURILLO DE LA CUEVA, señala que esta novedad, traída por la LOAP 41/2002, ya era anticipada en el artículo 10 del Convenio para la Protección de los Derechos Humanos y de la dignidad del ser humano con respecto a las aplicaciones de la biología y la medicina³⁹¹. Sobre el particular, coincido totalmente con el autor en este aspecto, pues aunque éste sea un caso excepcional, debe extremarse su uso, de forma tal que no se convierta en la norma general y se pierda el propósito del legislador al regularlo, fomentando a su vez el no reconocimiento del derecho que tiene el paciente y, además, como señala, será preciso estar especialmente atentos a la manera en que (sic) (como) se aplica y, desde luego, observar

³⁹¹ MURILLO DE LA CUEVA, Pablo L., “El derecho fundamental a la protección de los datos relativos a la salud”, en RIPOL CARULLA, Santiago (ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Marcial Pons, 2006, p. 37

criterios muy restrictivos a la hora de enjuiciar esa praxis para asegurar que únicamente se utiliza en situaciones límite.

Y es que la preocupación descrita por el autor tiene gran fundamento, pues si vamos a simples interpretaciones, se entraría mucho en el terreno de la subjetividad del médico que, aunque es interlocutor principal del paciente en lo referente a su atención e información durante el proceso asistencial, podría en un momento determinado desconocer el derecho que tanto se ha protegido al paciente, sobre su información de salud. Dicho lo anterior, si bien hemos sostenido que la LOAP 41/2002, cambia el rol paternalista³⁹² del médico, por una relación profesional, basada en la autodeterminación del paciente este permiso excepcional, raya en aquella característica casi superada, pues el profesional de la medicina, bajo condicionamientos culturales del principio de beneficencia y hasta supuestos de consideración subjetiva (cuya base es la ética del cuidado y de la comunicación no agresiva de la verdad, que aliente la confianza mutua y disminuya el sufrimiento), ante el estado delicado y débil del enfermo, se abroga el derecho de no participarle su situación, por entender que de hacerlo le haría más daño y estaría propenso a empeorar su condición de salud. Para usar este derecho, soy de la opinión que se debe tener mucho cuidado. Los pacientes actuales son más propensos a decidir sobre sus datos y, unidos a la tecnología, más

³⁹² Cfr., Así, TOMILLO URBINA, Jorge, “Nuevos derechos del paciente desde su condición jurídica como consumidor”, en Revista Derecho y Salud, Volumen 19, Extraordinario XVIII Congreso, pp. 43 – 54, señala que “en el sistema tradicional, el paciente desempeña un papel de sujeto – paciente como mero destinatario sumiso y obediente, desde el punto de vista social y desde el punto de vista existencial, a las órdenes e instrucciones “superiores” del facultativo”. Además, para el autor, en la profesión médica prevalecía un sentimiento de ayuda al enfermo, de tipo humanitario, derivado de la compasión que sentía el ser humano ante el sufrimiento y la enfermedad del paciente. En igual pensamiento está GALLEGO RIESTRA, Sergio, El derecho del paciente a la autonomía personal y las instrucciones previas: una nueva realidad legal, Aranzadi, 2009, p. 56, cuando dice que la sociedad moderna, a pesar de la fuerte implantación de los derechos individuales, con rango de derechos fundamentales en todas las cartas magnas, parece aceptar que el paternalismo lo impregna todo, estando presente, tanto en las relaciones del Estado con los ciudadanos como en las relaciones con las instituciones.

críticos con la información que se les da. Ahora no aceptan tan fácilmente imposiciones de terceros, lo que les hace muy diferentes a los de hace un siglo, cuando casi “todos los enfermos eran analfabetos e inseguros, y en consecuencia creían, sin rechistar lo que les decían los médicos, cuyo mérito principal, según las crónicas de ese entonces, era que sabían latín y apenas se les entendía la letra, que no deberían ser precisamente dos credenciales de efectividad”³⁹³.

Existen retos para el médico en este caso, como es aprender a detectar las necesidades y deseos de información, además de mantener una actitud dispuesta a compilar adecuadamente los datos y así determinar si la información que posteriormente debe facilitar al enfermo le afectará de forma negativa. Pensemos en los casos de trasplantes de órganos o de un cáncer terminal, con inicio de proceso de metástasis. Por otro lado, surgen para el médico aspectos de sumo cuidado: abrogarse el derecho a no informar al paciente, lo que es totalmente contrario a la práctica general, y por otro, comunicar datos de salud de su paciente a los familiares. Para esto hay que recordar que el dueño de la información siempre será el paciente y sólo serán informadas las personas vinculadas a él por razones familiares o de hecho, en la medida que el mismo paciente lo permita de manera expresa o tácita. Aquí ya empezamos a analizar la opción de ceder información de salud del enfermo, con la consecuencia para el médico de afrontar las consecuencias, si se demuestra que tal comportamiento no se ajusta a las excepciones que contempla la ley.

Siendo así, aunque este derecho está reconocido al personal médico y se le podría negar el acceso a los datos al propio paciente, no es menos cierto que tal derecho es una espada de Damocles que, en ocasiones, se moverá en algunos casos a favor del médico y en otras en su contra. No será para todos los casos. Por el contrario, se aplicará cuando sea el paciente quien manifieste expresamente su deseo de no ser informado, después se respetará

³⁹³ TOLOSA ASENJO, Miguel A., “Gestión hospitalaria y protección de datos médicos”, en RIPOL CARULLA, Santiago (ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Op. Cit., p. 121

su voluntad dejando constancia por escrito de su decisión, sin que esto implique un permiso abierto para todas las intervenciones médicas. Como es de lógica, también este derecho a no recibir información estará limitado por el interés de la salud del propio enfermo, de terceros, de la colectividad y por las exigencias terapéuticas del caso.

2.1.2. Otro tipo de accesos.

En principio, sólo el titular de los datos puede acceder a su información, mediante procedimiento que está formalizado, en aras de proteger su derecho. Tal como hemos visto en capítulos anteriores, existen casos especiales, definidos por la propia LOPD 15/1999 y su reglamento, en los que se puede acceder a los datos de salud sin el consentimiento del titular, casos con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia. Y en todos estos supuestos se exige, como mínimo, que quede asegurado el anonimato, a menos que el juzgado señale lo contrario o el interesado haya prestado su consentimiento para ello previamente.

Sin embargo, existen otros interesados que podrían demostrar su necesidad de acceder a los datos de salud, como son los agentes de inspección sanitaria, pero a éstos la ley sólo les recocerá cierto nivel de acceso “siempre que su finalidad sea la “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”³⁹⁴, mas no conocer en detalle la condición de salud del paciente. Aquí, se impone con fuerza la necesidad de coordinar los fines por los cuales se recogieron los datos con el interés mostrado por el tercero y, dado que estamos frente a datos especialmente protegidos, sería ilegal que alguien acceda a la información del paciente, sin el consentimiento del enfermo o con fines diferentes o incompatibles.

³⁹⁴ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0242-2010, p.6

Del mismo modo, este mismo informe jurídico señala que el acceso a la historia clínica, aún habilitado por lo previsto en su normativa específica reguladora, debe modularse en atención a la aplicación del principio de proporcionalidad en el tratamiento de los datos de carácter personal, consagrado por el artículo 4.1 de la LOPD 15/1999, debiendo limitarse el acceso a los datos que efectivamente resulten necesarios para el cumplimiento de los propósitos que justifiquen dicho acceso, sin que deba extenderse a datos no vinculados a dichos fines.

De esta manera, igual que en los casos del derecho a la intimidad, para los casos de los datos de salud, siempre se verificará el propósito que busca el tercero, para acceder a la información de salud del enfermo, entendiendo como base el fin principal de la historia clínica, que es dar seguimiento a la salud del paciente. Si no es el caso, debe negarse cualquier conocimiento por parte de extraños al enfermo.

2.2. La rectificación.

El derecho a rectificación y cancelación ha sido reconocido por la legislación estatal, mediante el artículo 16 de la LOPD 15/1999 y el artículo 31 del Real Decreto 1720/2007, de lo cual cabe decir que, aunque la legislación tienda a desarrollarlo en una misma sección, su contenido los hace totalmente diferentes entre sí. En el primero, se pretende corregir aquella información “errónea, inexacta o incompleta; y en la segunda, se pide la eliminación de los datos cuando se consideren inadecuados o excesivos”³⁹⁵. Por otro lado, ambos conceptos sí guardan vinculación en algunos aspectos, pues están relacionados con los principios que deben mantener los datos, reconocidos desde la Ley 5/1992, y consecuentemente por el artículo 4 de la LOPD 15/1999, en particular los de actualización, exactitud y conservación, siendo precisamente estos principios el fundamento para solicitar

³⁹⁵ PÉREZ DE VELASCO, José Ramón, “Protección de datos de carácter personal”, Revista Electrónica de Derecho Informático, núm. 27, 2000, p. 5

el ejercicio del derecho rectificación o cancelación, por su posible desconocimiento o incumplimiento. Por ejemplo, en casos de tratamiento de datos excesivos, la incompatibilidad de los datos frente al fin que justificó su recogida y/o tratamiento o cuando se haya excedido el periodo de conservación y no se haya procedido con la cancelación respectiva, siendo en consecuencia inexactos y violatorios de lo establecido por la LOPD 15/1999.

Asimismo, estos derechos tienen en común que ambos se constituyen en una alternativa efectiva para proteger al paciente, ya que “la divulgación de datos inexactos pueden atentar contra el honor de la persona cuando esa inexactitud la hace desmerecer en la consideración ajena”³⁹⁶. ORTI VALLEJO señala, con aguda claridad, que dicha inexactitud de los datos tiene varios efectos, más allá del impacto al honor de la persona, pues de darse alguna comunicación o revelación sobre datos inexactos o desfasados, también se podría influir negativamente en la personalidad del sujeto afectado, los cuales pueden desencadenar en el empeoramiento de su ánimo, su relación familiar y social.

En nuestra opinión, aunque “la transmisión de conocimientos, ideas e informaciones de unas personas a otras; es decir, el proceso de comunicación pública, se constituye, por ello, en el eje central de las relaciones sociales”³⁹⁷, resalta curiosa la necesidad que tienen las personas de corregir cualquier dato de salud que les pertenezca, especialmente por la reacción que genera ante la opinión popular. Existe una exigencia permanente de amoldarse a los parámetros de “aceptación” que impone la sociedad, de allí la necesidad que los demás no conozcan los datos de salud y, de hacerlo, por lo menos sean

³⁹⁶ ORTI VALLEJO, Antonio, Derecho a la intimidad e informática (tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada), Edit. Comares, p.164

³⁹⁷ NAVAS CASTILLO, Florentina, “Libertad de expresión y derecho a la información”, en TORRES DEL MORAL, Antonio (Dir.), Libertades Informativas, Colex, 2009, p. 89

los más exactos posibles, para no causar una deformación a la imagen que se tiene ante el resto de la sociedad y el rechazo sea lo menor posible. Del mismo modo, tal como afirma RUIZ CARRILLO, “la información es la representación de una realidad. Por definición, la información no tiene calidad; no es ni buena ni mala. Toda información es o no cierta y es o no verdadera”³⁹⁸, a lo que yo agregaría que, tal vez, la información pueda clasificarse de esa manera (verdadera o falsa), pero son los efectos que causan en el paciente y la sociedad los que se constituyen en buenos, malos y hasta terribles. Un enfermo puede padecer lepra³⁹⁹ (enfermedad casi extinta), y eso sería un dato cierto, pero son los efectos que produce los que definitivamente serían malos para él y malo para la sociedad que le rodea, por los riesgos de sufrir graves dolores y hasta la muerte, el rechazo sería una consecuencia inmediata y la exclusión sería la alternativa más recomendable para contener este tipo de enfermedad, sin importar que existan derechos que protegen al enfermo, aunque su patología tenga tales características infecciosas.

Por otro lado, sobre los principios generales de la protección de los datos, nos dice HERRÁN ORTIZ que “constituyen el contenido esencial del derecho a la protección de los datos y configuran un sistema de tutela que garantiza una utilidad racional y razonable de los datos personales”⁴⁰⁰. En esta misma línea, HEREDRO HIGUERAS señala que “la finalidad es el principio básico de la protección de los datos. Los demás son función de éste los datos deben ser pertinentes, adecuados y no excesivos con relación a la finalidad, deben ser exactos y

³⁹⁸ RUIZ CARRILLO, Antonio, Manual práctico de protección de datos, Edit. Bosh, 2005, p 18

³⁹⁹ La lepra fue históricamente incurable, mutilante y vergonzosa, al punto de que, entre otras medidas, se decretó en 1909, por demanda de la Sociedad de Patologías Exóticas, “la exclusión sistemática de los leprosos” y su reagrupamiento en Leproserías como medida esencial de profilaxis.

⁴⁰⁰ HERRAN ORTÍZ, Ana I, El Derecho a la protección de datos personales en la sociedad de la información, Universidad de Deusto, núm. 26, Bilbao, p.53 La autora también expone que es mediante estos principios que el legislador aspira a construir un sistema preventivo de tutela de la persona frente al tratamiento de sus datos, estableciendo un saludable equilibrio entre los avances de la sociedad de la información y el respeto a la libertad de los ciudadanos.

completos y actualizados en función de la finalidad y cancelados cuando hayan dejado de ser necesarios para la finalidad”⁴⁰¹.

Además, acorde con estos principios, se establecen una serie de obligaciones, “tendientes a alcanzar esa veracidad y exactitud de los datos de carácter personal que se encuentran en el fichero, y cuyo incumplimiento es digno de reproche”⁴⁰². En este sentido deriva en la imposición de sanciones, conforme a la gravedad de la actuación y la proporcionalidad que conlleva en dichos casos, pues en ocasiones la disminución en la culpabilidad o de la antijuridicidad de la conducta, puede llevar a fijar alguna escala en la cuantía de la sanción, aplicando criterios de conducta llevadas a cabo por el responsable del fichero.

Otro aspecto importante es que en la actual ley se habla de los derechos de rectificación “o” cancelación, dejando claro que son derechos independientes y que no es necesario primero rectificar y después cancelar. Esta delimitación no estaba⁴⁰³ tan clara en la Ley 5/1992, que hablaba de rectificación “y” cancelación, lo que usualmente hacía pensar la obligación de presentar dichos derechos en forma seguida y obligatoria.

La necesidad de ejercer el derecho a corrección puede implicar que el responsable del fichero no está cumpliendo cabalmente con una de sus obligaciones principales, que es mantener actualizado el dato. Si bien no resta oportunidad al paciente para presentar su solicitud, ésta, en principio, ni siquiera debe ser necesaria, si la información que se tiene del enfermo coincide con su actual estado de salud. Ahora bien, para hacer

⁴⁰¹ HEREDERO HIGUERAS, Manuel, La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal, Op. Cit., p.85

⁴⁰² SAN, de 17 julio 2006, FJ: 4 (JUR 2006\224860)

⁴⁰³ HERRAN ORTÍZ, Ana I, “El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales”, Dykinson, 2002, p.254

efectivo la reclamación, no basta con la simple manifestación de voluntad del paciente, a fin de lograr el cambio de sus datos en el fichero correspondiente. Además de esto, debe adjuntar las pruebas, en las que conste que efectivamente los datos de salud compilados a su nombre no son correctos o son incompletos. Y es el responsable del fichero quién determinará si tal información novedosa justifica hacer cambios en los ficheros existentes. En todo caso, corre por cuenta del interesado determinar qué datos son los incorrectos y cuál sería el reemplazo adecuado, tarea que se ve completada con la obligación del responsable del fichero en mantener actualizados todos los datos de salud que conserve del paciente. Para GARCÍA AMEZ, “la carga de la prueba de la falta del incumplimiento de este deber (actualización de los datos), recae en la persona que ejercita el derecho de rectificación, tal y como se deduce de la lectura de la norma tercera, en su punto 3, de la Instrucción 1/1998, que exige al interesado aportar la prueba documental de que justifique la necesidad de una rectificación de los datos”⁴⁰⁴.

A diferencia del plazo concedido por la LOPD 15/1999 y el Real Decreto 1720/2007 para el derecho de acceso, en el caso del derecho a rectificación el término es mucho más corto y sólo se conceden diez días al responsable del fichero para cumplir con la solicitud presentada por el paciente, teniendo la obligación no sólo de realizar los cambios solicitados, sino también comunicar, en aquellos casos que los datos hayan sido trasladados o cedidos a terceros, siempre cumpliendo con los requisitos de consentimiento previo y finalidad, la modificación realizada, a fin de garantizar que todos los ficheros que posee y de los cuales es responsable, correspondientes al pacientes, serán actualizados oportunamente. En esto último, se establecen estos plazos muy cortos, en razón del interés por los resultados y el respeto al derecho del paciente con su información de salud.

⁴⁰⁴ GARCÍA AMEZ, Javier, “La protección de datos del usuario de la sanidad: derecho a la intimidad y asistencia sanitaria”, en Revista Derecho y Salud, Op. Cit., p.60

Ahora bien, dado que estamos frente a supuestos en los que es el paciente quien solicita la rectificación, ésta igualmente estará condicionada a sólo su información, lo cual no implica una modificación en los datos que se conserven de terceros, y no debe alterar las “anotaciones subjetivas” que realizan el personal médico durante la atención que dispensa al paciente.

2.3. La cancelación.

La cancelación dará lugar a que se excluyan los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme al reglamento que establece el Real Decreto 1720/2007. En este aspecto también GARCÍA AMEZ señala que, “la cancelación viene vinculada con el principio del consentimiento, pues la persona, al ejercitar este derecho, ha decidido que sus datos no deben encontrarse registrados en un fichero, de modo que no se cuenta con el consentimiento del interesado, que recordemos es revocable en cualquier momento”⁴⁰⁵. Sobre lo anterior, estamos de acuerdo sólo en parte, pues es cierto que uno de los motivos que llevan al paciente a pedir la cancelación de los datos de salud, puede inspirarse en la falta de consentimiento, por todas las razones que no sería propio repetir en este momento. Sin embargo, en mi opinión, esta no sería la única razón que tendría, pues los datos desfasados y sin valor para los objetivos propuestos, bien pudieron ser recabados con el conocimiento y consentimiento del enfermo, pero después de un periodo de tiempo, determinado o determinable, podrían perder su vigencia, lo que los convierte en claros candidatos del derecho de cancelación, por no cumplir con los propósitos o fines iniciales de la recolección.

Volviendo al consentimiento, está justificado que sea voluntario y el paciente puede perfectamente cambiar de opinión y retirar la autorización para el uso de sus datos de

⁴⁰⁵ GARCÍA AMEZ, Javier, “La protección de datos del usuario de la sanidad: derecho a la intimidad y asistencia sanitaria”, en Revista Derecho y Salud, Op. Cit., 2010, p. 61

salud o su historia clínica por completo, en especial en aquellos casos en los que no se haya disociado el dato y se le pueda identificar junto con la patología que padece. Sin embargo, el bloqueo mencionado por la ley no implica un borrado total de la información, ya que debe conservarse a favor de las Administraciones Públicas, jueces y tribunales, en razón de las posibles reclamaciones que puedan derivar del tratamiento médico y “no siempre se procederá el borrado sino el bloqueo de los datos⁴⁰⁶, así sucederá respecto de aquellos que ya hubieran sido puestos a disposición de la autoridad judicial, sin perjuicio de la continuación del tratamiento respecto de los datos que fueran necesarios para garantizar la adecuada resolución de la causa”⁴⁰⁷. Por lo tanto, aunque por regla general debe procederse a la cancelación de los datos, al ser éstos innecesarios para la finalidad que justificó su tratamiento o por haberse cumplido los fines que relacionan al responsable del tratamiento con el paciente, dicha cancelación deberá producirse mediante el bloqueo de los datos de carácter personal sometidos a tratamiento que, produciendo unos efectos similares al borrado físico de los datos, no serán borrados totalmente del sistema, al amparo de la legislación para el caso en particular.

Igualmente, se pide claridad al paciente sobre qué datos debe cancelar y debe, además, presentar las justificaciones para tal petición, lo que también será evaluado por el responsable del fichero, dentro del término común de diez días para proceder a la cancelación de los datos, de ser posible y comunicar igualmente a todos a quienes se haya cedido la información, a fin de que procedan al bloqueo correspondiente.

Para proceder con la cancelación, el responsable del fichero debe atender varios elementos, antes de bloquear los datos de salud del paciente. Por un lado, debe verificar si la

⁴⁰⁶ El bloqueo deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que usualmente los consultaba, en los casos de los pacientes, deberá estar bloqueado para terceros no autorizados por el titular de los datos.

⁴⁰⁷ AGENCIA DE PROTECCION DE DATOS, Informe Jurídico 0156-2010, p. 4

vigencia de tales datos no está condicionada a contrato previo realizado con el paciente, precisamente para acumular los datos por determinado periodo de tiempo de ser así, no podrían cancelarse los datos de manera inmediata y debe cumplir con procedimiento especial que determine el derecho que asiste a las partes.

De otro lado, dado que estamos frente a historiales clínicos, sobre los que existe una ley estatal que desarrolla de manera especial su conservación, debemos entender que en estos supuestos existe una limitación legal al derecho de cancelación, que ya no operaría por simple voluntad del paciente, sino que tendría que ajustarse a los plazos establecidos por la ley. Esta situación también se apoya en la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, en el apartado 5 de su norma tercera establecía que “la cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos”.

De esta manera, surge nuevamente la obligación de determinar cuál es el tiempo que deben conservarse los datos de salud que contiene una historia clínica, la LOAP 41/2002, si que establece un término “mínimo”, que se fija en cinco años, pero reconoce a su vez que esta materia podrá desarrollarse de manera privativa a las comunidades autónomas para ampliar este plazo, conforme a sus propias necesidades. Además, de acuerdo al art. 17.2 de la LOAP 41/2002 estos datos de salud también deben conservarse a efectos judiciales, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud, aunque para estos casos, su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas. Sobre el particular, algunos autores⁴⁰⁸ señalan que este plazo básico de cinco años puede resultar complicado cuando se trata de exigir responsabilidades civiles o penales, ya que parece muy

⁴⁰⁸ PALOMAR OLMEDA, Alberto, “Confidencialidad y protección de datos en la ley de salud sexual y reproductiva y de interrupción voluntaria del embarazo, cuatro estudios”, en Revista Derecho y Salud, Op. Cit. p. 77

restrictivo en relación con la prescripción de las acciones y los delitos, en otro extremo, señalan que hacerlos acorde con los plazos civiles o penales también haría muy compleja la gestión documental y de archivo. Sobre lo anterior, creo que mientras mayor sea el plazo, más garantías hay para el paciente en caso de presentar una reclamación, ya que las consecuencias de un mal tratamiento no siempre se muestran de inmediato en la salud del paciente, y pueden tener etapas de evolución lenta. Por otro lado, los plazos amplios “no complicarían” la gestión documental, a menos que se realice solamente de forma física, pues con el apoyo de las nuevas tecnologías y la digitalización documental se puede lograr el archivo de grandes volúmenes de documentos e información, sin ocupar gran espacio, exceptuando evidentemente las muestras biológicas y de tejidos, que por su propia naturaleza, perecen en un tiempo determinado, si no se les brinda la conservación pertinente.

Está claro entonces que existe la necesidad de conservar los datos de salud en forma adecuada y segura, para proteger la confidencialidad de la información y garantizar los derechos fundamentales de los pacientes, asimismo, la obligación de que los datos relacionados con su salud puedan ser adecuadamente conocidos por los facultativos que pudieran tratarles. Esto último “supone que los datos contenidos en la historia clínica, en cuanto se relacionen con la salud del individuo y su consulta resulten adecuados para preservar dicha salud, deberán conservarse durante el tiempo adecuado a cada caso, obviamente según criterio médico, no procediendo cancelar dichos datos cuando pudiera perjudicarse la salud futura del paciente al que se refieren los mismos, sin olvidar otros intereses legítimos de terceros, presentes con frecuencia en materia de salud, y el resto de usos admitidos en la LOAP 41/2002 ya citados y en la normativa de sanidad”⁴⁰⁹. Más allá de estos casos, resulta difícil establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, los plazos de prescripción de las acciones que pudieran “derivarse de la relación jurídica que vincula en el contrato, así como los derivados

⁴⁰⁹ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0049-2005, p. 3

de la normativa tributaria o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia LOPD 15/1999, en relación con las conductas constitutivas de infracción muy grave⁴¹⁰.

Y es que en estos casos de cancelación de datos de salud, el artículo 16.2 de la LOPD 15/1999 no prevé una cancelación automática de los datos por la mera petición del afectado sino que reserva este derecho para aquellos casos que no se ajusten a la ley. En sí, el Informe Jurídico 0189- 2003 de la Agencia de Protección de Datos, señala que hay determinados supuestos en los que “la ley legitima o incluso impone el tratamiento y no será posible acceder a la cancelación de los datos fundada en una mera solicitud del afectado. Así, por ejemplo, el interesado no podrá pretender la cancelación de los datos necesarios para el mantenimiento de una relación contractual⁴¹¹ con el responsable del tratamiento o de

⁴¹⁰ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0339-2008, p. 6

⁴¹¹ De este modo hay que resaltar que aunque el derecho de cancelación existe a favor del paciente, esto no supondrá el desconocimiento de obligaciones contractuales previamente establecidas con el hospital responsable de sus datos, por lo que no cabría una solicitud de cancelación de los datos de salud, por encima de saldos o deudas pendientes por cancelar en razón de tratamientos médicos brindados, ni se puede amparar la negativa a recibir el cobro, por haber solicitado previamente la cancelación de sus datos. En caso parecido, resolvió la SAN, de 29 abril de 2011, FJ: 4 (JUR 2011\165379) y que señala que la entidad recurrente, después de haberle comunicado al interesado que accedía a la cancelación y bloqueo de sus datos personales, le reclamó una deuda derivaba de su previa relación contractual y que al parecer había resultado impagada. El hecho de que Endesa al acceder al derecho de cancelación no especificase que dicha cancelación solo produciría efectos "pro futuro", tanto para dar por concluida la relación comercial que les vinculaba como para la futura remisión de publicidad u otro tipo de tratamiento de sus datos futuros, no podía ser interpretado como la imposibilidad de utilizar los datos del recurrente para reclamarle deudas vencidas y exigibles correspondientes al periodo en que la relación comercial entre ambos subsistía, otra interpretación de esta comunicación debe reputarse absurda y desproporcionada. El derecho de oposición y cancelación de datos no puede ser utilizado como mecanismo liberatorio o de condonación de deudas vencidas y, por ende, la entidad Endesa se encontraba autorizada a seguir tratando los datos personales del cliente con la finalidad de reclamarle las deudas pendientes.

aquéllos que el responsable está legalmente obligado a mantener”⁴¹². Esta conservación del dato bloqueado también sirve para que la autoridad pueda determinar con exactitud si existió o no un previo tratamiento del dato de salud o si el responsable del tratamiento, procedió adecuada y oportunamente con su cancelación, en los plazos impuestos por la ley. Para esto no es necesario crear un nuevo fichero con los datos “bloqueados”, sino que basta con hacer las anotaciones pertinentes, que impidan que dicha información sea accesible y se prevea un mecanismo de control sobre las personas que tendrían conocimiento posterior de dicha información de salud. Al evitar la duplicidad del fichero con la creación de uno nuevo, no habría necesidad de informar nuevamente a la Agencia de Protección de Datos, por la generación de un fichero distinto al anterior.

Por otro lado, aunque el concepto de fichero no va directamente vinculado a la exigencia de que el mismo se encuentre en una única ubicación, esto es de por sí una diferencia sustancial con el concepto general de la historia clínica que hemos reiterado en páginas anteriores. No parece incompatible con la ley, la existencia de varios ficheros parecidos, distribuidos en lugares geográficos remotos entre sí, “siempre y cuando la organización y sistematización de los datos responda a un conjunto organizado y uniformado de datos, sometido a algún tipo de gestión centralizada”⁴¹³. Al igual que en los casos anteriores, el responsable del fichero tendrá que justificar razonadamente por qué no concede el derecho de cancelación y advertir al paciente los derechos que le asisten en caso de no sentirse conforme con la decisión. También debemos reconocer que la propia ley establece supuestos en los que estos derechos no pueden ser concedidos, como es el caso del artículo 23 de la LOPD 15/1999, cuando los datos recogidos tienen fines policiales “en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.”

⁴¹² AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0189 -2003, p. 2

⁴¹³ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0368 – 2003, p.1

Más curioso es el análisis que hace algún autor⁴¹⁴ sobre la facultad que tiene el Responsable del Fichero de cancelar los datos de una persona, de forma oficiosa, sin que medie consentimiento del interesado. Afirma que aunque el legislador habla de la facultad de sustituir de oficio los datos “a lo mejor quiso decir y no dijo” que los datos podían ser cambiados (entendiendo también un borrado de los datos anteriores). En este aspecto señala que actualizar los datos no necesariamente implica sólo reemplazar uno nuevo por uno viejo y borrar el dato viejo. Por el contrario, bastaría con enviar el dato reemplazado a un histórico y así conservar toda la información que se tiene de la persona. Deduzco que al autor le interesa resaltar la necesidad de mantener una secuencia de la información, de forma tal que se pueda ver cómo han evolucionado los datos, sin perder el génesis por culpa de la actualización de los datos que se consideran novedosos y ajustados a la situación actual de la persona.

Así, pone de manifiesto un ejemplo con los registros escolares, en los que se pueden actualizar los datos de domicilio y número de teléfono de los alumnos, sin llegar al borrado total de la información anterior. Nosotros igual ajustaríamos tal ejemplo al de los historiales de salud, en los que también se actualizan datos constantemente y se requiere mantener un hilo histórico, que muestre los cambios que ha tenido el paciente en sus datos generales y demás durante cada momento de su asistencia. Lo que no podría compartir del todo es que sólo el afectado pueda ordenar la cancelación de los datos, debido a que esto a su vez es una obligación del responsable del fichero, y que consiste en mantener los datos actualizados y vigentes por el término que establece la ley. Pensemos en aquellos casos en los que se ha cumplido el plazo mínimo de 5 años para conservar los historiales clínicos. No se podría pretender que se deba obtener el consentimiento o la petición del paciente, para después proceder a la cancelación de la información. Esto, más que un respeto al derecho del paciente, podría convertirse en un obstáculo para la realización de las tareas diarias con la

⁴¹⁴ RUIZ CARRILLO, Antonio, Manual práctico de protección de datos, Bosh, 2005, p.27

dificultad de no ser eficiente en su gestión, que igual no concuerda con los propósitos que están obligados a cumplir.

Lo que si es de meritorio reconocimiento es la obligación del responsable del fichero, en el evento que proceda a una rectificación o cancelación de los datos de forma oficiosa, a dejar constancia de los cambios realizados en el fichero, con especial énfasis en cómo obtuvo la información actualizada y desde cuándo procede a su reemplazo, de forma que el paciente pueda conocer cómo se hicieron los cambios a sus datos y a partir de qué fecha puede entenderse que dicha información forma parte de los datos que se mantienen de su persona y posiblemente se haya utilizado por terceras personas, mediante el proceso de cesión de información.

De igual forma, entendemos que no toda actualización implica por un lado borrar el dato anterior, ni la sustitución por uno nuevo, lo que podría denominarse un reemplazo de los datos, pues también existirán los casos de datos que complementan una información previamente entregada por el paciente. Por ejemplo, un paciente que posteriormente incluye, además de su dirección fija, una dirección diferente para casos especiales, ambos estarían dentro del renglón “dirección de paciente”, y serían igual de importantes. A la vez, podríamos tomar como ejemplo en los historiales clínicos los datos de los familiares que en un primer momento se entregan con las generales más básicas, pero que después pueden ampliarse con información más completa. En esos casos, la información nueva no desplaza la anterior a una sección histórica, sino que se reúnen entre todas para lograr una mayor exactitud en la realidad del paciente.

2.4. El derecho de oposición.

Es lógico que si el derecho a controlar el uso de la información de salud del paciente se considera un derecho libre, sujeto a la voluntad, también en algunos casos exista

la posibilidad de oponerse a que terceros hagan uso libre de esta información. Así, el Real Decreto 1720/2007, contempla este derecho en su artículo 34, y lo define como el “derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo...”. El reconocimiento del derecho de oposición en la Directiva 95/46/CE, del PE y el CUE facilitó su incorporación al texto español; de suerte que si bien no puede decirse que la LOPD 15/1999 siga fielmente en este punto las previsiones comunitarias, “al menos puede asegurarse que su configuración contribuye a reforzar los fundamentos de la protección de los datos en el ordenamiento español”.⁴¹⁵

En este derecho, lejos de corregir algún dato, como vimos en el apartado anterior, el paciente expone su negativa a que se incorporen sus datos de salud en un fichero determinado, a la luz de las posibles desventajas que tal incorporación le acarrearán, por no decir trato diferente y hasta discriminatorio. El derecho a oposición en el uso de los datos también encuentra amparo en la Directiva 95/46/CE, del PE y el CUE, puesto que su artículo 14 reconoce este derecho, en especial el apartado “b”, que establece que “el interesado tendrá derecho a oponerse previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización”.

Ahora bien, a primera vista de lectura de este artículo se podría dudar sobre el concepto “el afectado”, por ser personaje indeterminado, que bien podría ser el paciente o sus familiares, o persona distinta que sienta que la información planteada en el fichero tiene efectos negativos y que por consiguiente le acarrea las desventajas mencionadas. Esta

⁴¹⁵ HERRAN ORTÍZ, Ana I, El derecho a la protección de datos personales en la sociedad de la información, Op. Cit., p.58

indeterminación al utilizar el posesivo “sus”, para dejar claro que no se trata de otra persona, sino sólo aquella a quien pertenezcan los datos, en este caso de salud. Existirán entonces dos tiempos para ejercitar este derecho: durante el proceso de incorporación de los datos en el fichero, que sería un momento “previo”, no habría un riesgo de su tratamiento o de su cesión por no perfeccionarse el proceso de captación de la información; y un segundo tiempo, que estaría determinado por el cese en el uso, una etapa “posterior”, en los que sí pudiese existir el riesgo de que los datos hayan sido utilizados, cedidos o que existan ya las consecuencias negativas.

En todo caso, el uso del dato no sería el mayor de los problemas para el afectado, sino las consecuencias que se derivan de éste, en especial, si no cuentan con el consentimiento previo y se pretenda justificar su uso para propósitos diferentes o lesivos a los intereses del paciente, sin que sean autorizados por una norma con rango de ley.

Estos tipos de derechos igual deben ejercitarse, en primer término, ante el responsable del fichero, con las pruebas o justificaciones que sustenten su petición, y se tendrá un término de diez días para resolver lo pedido. Aunque igual que en los casos anteriores, el responsable del fichero tendrá a cargo determinar si las justificaciones presentadas por el paciente son suficientes para proceder a la suspensión en el proceso de captación de los datos en el cese de su uso. Aun así, tampoco el paciente quedará desprotegido, pues le queda la tutela de la Agencia de Protección de Datos, Estatal o Autonómica, según sea el caso, para revisar la decisión tomada por el responsable del fichero, previo proceso administrativo para dicha causa.

Sumado a lo anterior, el Real Decreto 1720/2007 establece, en su artículo 36, un tipo de oposición, a la que denomina derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos. En este tipo de casos incorpora la figura de “los interesados” para referirse a quienes se vean afectados por la toma de decisión

con base en la información obtenida únicamente de los ficheros, sin participación de la persona dueña de la información. Es más, se refiere una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, de lo cual se podrían deducir varios extremos.

El Real Decreto 1720/2007, en su artículo 36.1 establece que los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta la decisión conlleve efectos jurídicos. De ahí que la norma se refiere a una afectación evidente, en desmejora del titular de la información, condición que se impone precisamente por extraer perfiles de personalidad de los datos personales.

Sobre la personalidad, nos dice HERRAN ORTÍZ que la obligación del responsable del fichero no puede ni debe quedar restringida a ofrecer información al interesado sobre los criterios de valoración y programas utilizados en el tratamiento y en la decisión, sino que dicha información ha de constituir un paso previo e ineludible para el responsable del fichero, de suerte que ofrezca al interesado los elementos de juicio y valoración para después poder impugnar los actos y decisiones que le perjudicaban y se han basado en esas valoraciones⁴¹⁶”. La autora amplía sobre este tema y señala que esta prescripción debe tomarse como un complemento ineludible, tanto como una condición sine qua non, pues permite al interesado poder ejercitar el derecho de impugnación que la ley le reconoce, ya que sin ello estaría frente un recurso sin eficacia.

⁴¹⁶ HERRAN ORTIZ, Ana I., El Derecho a la intimidad en la nueva ley orgánica de protección de datos personales, Op. Cit., p. 249

En fin, en nuestro tema, podría ser el caso de un paciente que no se beneficie de determinados tratamientos, dado que previamente se han utilizado ilegalmente datos de su historial, para cambiar su estatus, en consecuencia, no podrá usar tales derechos, o que le apliquen algún despido por la cantidad de bajas que acumula en un periodo determinado, sin que se le haya pedido permiso para utilizar dicho registro de inasistencia para temas de evaluación de trabajo.

La propia norma establece que el derecho a oposición cobrará mayor fuerza en los casos en los que se utilicen los datos (de salud) para propósitos comerciales o publicitarios⁴¹⁷. Así, la LOPD 15/1999 señala, en su artículo 30.4, que los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

En resumen, todos estos derechos ARCO son independientes y no se exige que deban presentarse de forma concatenada para que tengan validez. De hecho, aunque el derecho de acceso tiene como finalidad conocer si existe efectivamente un tratamiento de datos en relación con la persona concreta, esto no impide que, si el afectado tiene certeza de que sus datos se están tratando, pueda interponer directamente su derecho a rectificación o cancelación, en el caso en que dichas acciones procedan.

De igual forma, estos derechos ARCO son reconocidos, inclusive para aquellos casos en los que no se requiera el consentimiento, tal como lo establece el artículo 10.2.a del Real Decreto 1720/2007, cuando se refiere al tratamiento o la cesión que tengan por objeto

⁴¹⁷ La Ley 34/1988, de 11 de noviembre, General de Publicidad define en su artículo 2 esta actividad como: “Toda forma de comunicación realizada por una persona física o jurídica, pública o privada en el ejercicio de una actividad comercial, industrial, artesanal o profesional, con el fin de promover de forma directa o indirecta la contratación de bienes muebles o inmuebles, servicios, derechos y obligaciones”

la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por una norma con rango de ley, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la LOPD 15/1999. De este mismo artículo 10, tenemos que señalar que se ha procedido a la anulación del apartado 10.2.b⁴¹⁸, por considerar el Tribunal Supremo que excede el desarrollo del artículo 7.j de la Directiva 95/46/CE, del PE y el CUE, que establece únicamente dos requisitos acumulativos para que un tratamiento de datos personales, sin consentimiento del interesado, sea lícito. A saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado, en si, este alto Tribunal ha procedido a la anulación, dado que el artículo 10.2.b, además de los requisitos antes señalado por el artículo 7.j, exigía que la informaciones que no contaran con el consentimiento del interesados, debían obtenerse de fuentes accesibles al público⁴¹⁹delimitando exclusivamente qué documentos poseen esta característica. Ante

⁴¹⁸ Así la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), interpuso recurso contencioso administrativo contra el Real Decreto 1720/2007, el cual fue admitido por la Sala. Los denunciantes piden que, mediante trámite judicial, se declare la nulidad y dejen sin efecto algunos preceptos del reglamento de desarrollo de la LOPD 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre; se condene en costas a la Administración, conforme dispone el art. 139.1 de la Ley reguladora de este orden jurisdiccional; y se plantee cuestión prejudicial ante el Tribunal de Justicia de las Comunidades Europeas, con suspensión del recurso en tanto no recaiga sentencia por parte del citado Tribunal, proponiendo varias consultas. Este proceso, después de contar con la respuesta del Tribunal de Justicia de las Comunidades Europeas, sobre las consultas prejudiciales, culminó en sentencia del Tribunal Supremo de 8 de febrero de 2012, en lo que se extendió el pronunciamiento de estimación del recurso contencioso administrativo contra el Real Decreto 1720/2007, de 21 de diciembre, que se realizó en sentencia de 15 de julio de 2010, y se anuló el artículo 10.2.b) del Real Decreto en mención, por ser disconforme a derecho, sin hacer especial condena en costas.

⁴¹⁹ Se consideraba en el Real Decreto 1720/2007, artículo 10.2.b, como información de acceso al público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa

esta situación, a criterio del Tribunal y que no comparte el Abogado del Estado⁴²⁰, tal exigencia no actúa como elemento de ponderación y ninguna dificultad de redacción habría para darle ese carácter. Ya algunos autores⁴²¹, antes de la emisión de esta sentencia, habían señalado su preocupación, pues consideran que se encuentran ante un supuesto que pone en entredicho una cuestión central del régimen jurídico de los datos en España. La aceptación de la cuestión prejudicial supone “una apertura” del régimen garantista español que estaba centrado, hasta el momento, en el consentimiento o la determinación de la ley como elementos centrales de la gestión del dato. Igualmente, esta tesis no puede ser más que compartida, pues considero que además se impone una limitación al desarrollo normativo interno, al reducir la capacidad de incluir más garantías al ciudadano, por encima de la reglamentación básica que promueve la normativa comunitaria.

Ahora bien, también es muy importante que cuando el interesado solicita el acceso a sus datos en un fichero que se nutre de datos obtenidos de fuentes accesibles al público, el responsable del fichero o del tratamiento deberá extremar las precauciones para facilitar la información completa puesto que es la única forma de saber si obran datos suyos en tales ficheros y poder ejercitar el derecho de cancelación. En definitiva, de no requerir el consentimiento, bajo amparo de la LOPD 15/1999 o de su Reglamento, “esto no supone que

específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación, artículo que fue anulado mediante STS, del 8 febrero 2012, FJ: 7 (JUR\2012\62074)

⁴²⁰ En cuanto a este artículo, el Abogado del Estado, sostiene que es viable su redacción, ya que se basa en el desarrollo armónico del artículo 6.2 de la LOPD 15/1999 que excepciona de la necesidad del consentimiento del interesado, previsto en el apartado 1, como regla general, para el tratamiento de datos de carácter personal, entre otros supuestos, cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se le comuniquen los datos, siempre que no se vulneren los derechos fundamentales del interesado.

⁴²¹ PALOMAR OLMEDA, Alberto, “Confidencialidad y protección de datos en la ley de salud sexual y reproductiva y de interrupción voluntaria del embarazo, cuatro estudios”, en Revista Derecho y Salud, Op. Cit. p. 71

el afectado quede privado de otros derechos que le son reconocidos en dicha ley”⁴²², en los cuales se puede apoyar si se siente afectado por terceros.

2.5. Los derechos ARCO y los herederos del paciente.

He señalado que estos derechos de acceso, rectificación y cancelación, están dentro de los derechos que deben ejercerse de manera personal por el afectado, y que la decisión de ejecutarlos no puede transferirse a terceros distintos al titular del derecho. Aun son de interés las decisiones que se han tomado en los casos del heredero que desea acceder a un fichero en el que constan datos de salud de un familiar que ha fallecido o, por lo menos, corregirlos. Sobre el particular, la Agencia de Protección de Datos⁴²³ ya analizó si la muerte de las personas da lugar a la extinción del derecho a la protección de datos, con base al artículo 32 del Código Civil que dispone “la personalidad civil se extingue por la muerte de las personas”, lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad.

En si, bajo este criterio se han emitido resoluciones, entre ellas la de 23 de mayo de 2006, recaída en el procedimiento E/779/2005 y la resolución de 12 de junio de 2007, dictada en el expediente E/344/2006, y ambas tienen en común que “la LOPD 15/1999 tiene por 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, según dispone en su artículo 1”. luego entonces, las personas fallecidas no son titulares del derecho a la protección de datos de carácter personal y el derecho reclamado por los herederos queda al margen del ámbito de aplicación de la LOPD 15/1999, ante la inexistencia de sujeto de derecho, quedándoles solamente la opción a las personas vinculadas al fallecido, por razones familiares o análogas, dirigirse a los

⁴²² AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0593 -2009, p. 2

⁴²³ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0061-2008.

responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo y solicitar, cuando hubiere lugar a ello, la cancelación de los datos, en virtud del artículo 2.4 del Real Decreto 1720/2007. Con esto, la Agencia plantea que se “logra conciliar el carácter personalísimo del ejercicio de los derechos de acceso, rectificación, cancelación y oposición con la posibilidad de que el responsable conozca efectivamente el hecho mismo del óbito y pueda proceder, en su caso, a la cancelación de los datos, evitando a la vez situaciones que pudieran llegar a resultar incluso dolorosas para los allegados a un fallecido y que se derivarían del hecho de desconocerse esta circunstancia por parte de quien trata los datos, sin que ello implique en ningún caso el ejercicio por los herederos que la LOPD 15/1999 reserva exclusivamente al causante ya fallecido”⁴²⁴.

Es importante recordar, como ejemplo, los criterios esbozados por el Tribunal Constitucional⁴²⁵ cuando reconoció el derecho a la protección de la intimidad familiar, mencionado en capítulos anteriores. El Tribunal Constitucional señaló que, aunque el derecho fundamental a la intimidad es un derecho personalísimo que se extingue con la muerte, puede existir una afectación a los familiares y por ende no estaría alejado del Derecho que en estos casos especiales los familiares o análogos puedan pedir el respeto al derecho a la intimidad del fallecido. Siendo así, creo que sería interesante analizar si estos mismos principios pueden aplicarse para los casos del derecho fundamental a la protección de los datos, por considerarlos casos también especiales, y permitir ejercitar los derechos ARCO a los herederos de los pacientes, si demuestran que existe una afectación a sus intereses, que justifique tal petición.

No con esto dejo de lado el reconocimiento que ya existe en el Real Decreto 1720/2007, para los casos de cancelación, pero no es menos cierto que parece que,

⁴²⁴ AGENCIA DE PROTECCIÓN DE DATOS, Informe Jurídico 0061-2008

⁴²⁵ STC, 231-1988, de 2 de diciembre, FJ: 4 (RTC 1988/231)

excluyendo los derechos de rectificación y cancelación, los otros derechos no son reconocidos a los herederos. Para TRONCOSO REIGADA, todas las personas (vivas o muertas), tienen derecho a la protección de los datos y, a su juicio, el Real Decreto 1720/2007 no puede limitar la titularidad de un derecho fundamental si esto no lo ha manifestado expresamente la ley⁴²⁶. Señala además que no parece razonable reconocer el derecho al honor, a la intimidad personal y familiar y a la propia imagen a las personas fallecidas y negarles el derecho fundamental a la protección de datos personales, que es también un derecho de la esfera personal y que se constituye muchas veces como garantía del derecho a la intimidad. Mucho menos que esta limitación se haga mediante un reglamento, cuando la titularidad de un derecho fundamental está sometida a reserva de la ley orgánica.

En consideración parecida, pero no igual, se muestra NICOLÁS⁴²⁷, ya que hace referencia a la protección especial que merecen los datos genéticos, por no tener una afectación individual, tal como se ha reconocido al derecho a la intimidad. La autora también señala que este reconocimiento “familiar”, no significa que se identifique a un sujeto de derecho distinto del individuo, ni que con este supuesto un miembro de la familia pueda inmiscuirse en la información reservada de otro miembro. Asimismo, deja sentado que, en el caso de los datos genéticos del fallecido, desaparece el sujeto del derecho, pero subsiste un objeto sobre el que se puede ostentar un interés que, en su caso, debería ser protegido

⁴²⁶ TRONCOSO REIGADA, Antonio, Protección de datos personales para servicios sanitarios públicos, Agencia de Protección de Datos de la Comunidad de Madrid, Thomson, 2008, p.27. El autor destaca que el artículo 3 de la LOPD 15/1999, define como “datos de carácter personal” como cualquier información concerniente a personas físicas identificadas o identificables, no estableciendo como exigencia que las personas estén vivas. Así, dice que una persona fallecida es, ha sido, una persona física, no una persona jurídica. Además, el artículo 1 de la misma LOPD 15/1999 señala que esa ley tiene por 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.

⁴²⁷ NICOLÁS, Pilar, “El Concepto de dato médico y genético”, en RIPOL CARULLA, Santiago (ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Op. Cit. p. 95 y 96

aunque es cierto que “los derechos a la personalidad se extinguen con la muerte, pero, por otra parte, existen razones que justifican la necesidad de establecer normas de protección de la información genética del fallecido”⁴²⁸. Sobre lo anterior, entiendo que se promueva esta tesis, debido a que el sobreviviente está vinculado con la información genética que subsiste de su familiar fallecido, y eso le permite tener un interés legítimo en tener acceso a la información, pero creo que, de igual manera, siendo muy amplios, también se les debería reconocer los derechos de corrección y cancelación a los datos de salud en general del fallecido, por estar relacionados indirectamente con los familiares sobrevivientes, aunque eso no los convierta en propietarios de los mismos, salvo casos muy excepcionales (gemelo monocigótico).

3. La obligación de callar los datos de salud.

Antes de que se consolidara el derecho a la protección de los datos y se hablara de un derecho puro del paciente, existían las bases para la protección de la información de salud y la intimidad, especialmente en la atención médica. Así, correspondía esta gran tarea al médico, como garante y protector de la información entregada por su paciente, la cual sería resguardada bajo esa relación profesional que existe entre el enfermo y su médico. Esta peculiar relación según el modelo tradicional, también se basa en “el principio de confianza, desde cuya perspectiva, aquél no es sino un acto de beneficencia que el facultativo realiza con entrega inspirado por la idea de hacer el bien de forma altruista”⁴²⁹.

⁴²⁸ NICOLÁS, Pilar, “El Concepto de dato médico y genético”, en RIPOL CARULLA, Santiago (ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Op. Cit. p. 99

⁴²⁹ TOMILLO URBINA, Jorge, “Nuevos derechos del paciente desde su condición jurídica como consumidor”, en Revista Derecho y Salud, Volumen 19, Extraordinario XVIII Congreso, p.45. Este autor también desataca el sacrificio extraordinario que dispensaba el médico, desde inicio del trato de las enfermedades, carga que soportaba por encima de su derecho a diversiones, descanso, incluso vida familiar. Además del riesgo evidente

De esta manera, como consecuencia de la elaboración de la historia clínica y de la protección al derecho a la intimidad, surge un deber especial para los profesionales de la medicina: el ser garantes de los secretos que le han sido confiados por el paciente. En si, este tipo de secreto, constituye la obligación que tienen todos los que ejercen una profesión, a mantener en reserva la información que se les ha entregado en razón de su oficio. Esto es así, pues el ejercicio de muchas actividades profesionales implica, necesariamente para quienes las desempeñan, el tener que saber o conocer, de parte de sus clientes, algunos aspectos de su vida privada, pública o comercial, que asumen la calidad de íntimos y que, por lo mismo, les preocupa que sean revelados o conocidos por terceros. Se hacen dichas confidencias por la sencilla razón de que son imprescindibles para que el profesional pueda entender la dimensión del problema y responder en forma apropiada a la expectativa de solución que se le pide.

El Tribunal Supremo señala que “los derechos fundamentales realmente protegidos mediante el secreto profesional, son los derechos al honor, a la intimidad personal y familiar y a la propia imagen, conceptos cuyo contenido esencial está constituido por valores inmateriales, pertenecientes al fuero de la conciencia individual, como pone de relieve el catálogo de intromisiones ilegítimas del art. 7 de la Ley Orgánica 1/1982, básicamente fundadas en el sentimiento subjetivo de quien las padece al ver desvelada su intimidad o puesta en entredicho su reputación y buen nombre, desmereciendo o creyendo desmerecer en la consideración ajena”⁴³⁰. No hay duda que un profesional que no proteja las confesiones de sus clientes, mal podría ser una garantía como un “trabajador responsable”, a quien se pueda recurrir cuando sea necesario.

al contagio, dada la relación de proximidad que implica la profesión médica y que está sometida a altos niveles de riesgo.

⁴³⁰ STS, de 2 de julio de 1991, FJ: 4 (RJ 1991\6219)

Si en todas las profesiones existe el secreto profesional, en el sector sanitario se adquiere un grado de máxima importancia, ya que el médico, de acuerdo al artículo 10.3 de la LGS 14/1986, es un confidente necesario, pues no sólo es depositario de las más íntimas manifestaciones del cuerpo sino también las del fuero interno de cada sujeto, pues se le comparten no solo las dolencias físicas, sino también un cúmulo de pensamientos y sentimientos que son íntimos de un enfermo. De lo contrario, estas personas no hubieran venido a contar su historia o a mostrar su cuerpo. No obstante, aun quedan pendientes de clarificación sus límites, pues los avances médico/tecnológicos marcan un ritmo difícil de seguir para la normativa sanitaria, que cada día se queda obsoleta frente al cambio frenético de la ciencia.

Siendo así y entrando en materia, para MUÑOZ CONDE, el secreto médico es concebido originalmente como una especie de obligación y casi privilegio profesional, que se le debe considerar hoy desde el prisma del derecho a la intimidad del paciente, siendo objeto de amplias regulaciones⁴³¹. En si, constituye aquellas revelaciones que, por razón de profesión, el médico reciba de sus clientes, conducentes a recibir a cambio un consejo o servicio correspondiente a esta profesión⁴³². Como quiera que callar y no hablar serían consecuencias dimanantes del secreto médico, está claro que acogerse a un derecho de no hablar ha sido uno de los aspectos más controvertidos pues a diferencia de la profesión del abogado, por ejemplo, el médico si tendría que develar la información que protege, si es requerido por autoridad judicial. En esencia, podrá existir obligación de los profesionales a informar cuando sea requerido por la autoridad, por ejemplo la Administración Tributaria, pero en términos generales, el deber de informar no podrá abarcar a cuestiones de índole o naturaleza no patrimonial cuya revelación puede atentar contra el derecho a la intimidad personal, familiar o propia imagen⁴³³.

⁴³¹ MUÑOZ CONDE, Op. cit., p. 267

⁴³² Disposición deontológica, número 23 de la Orden del Ministerio de Gobernación, 8 de septiembre 1945

⁴³³ STSJ de Madrid, 939-2000, de 14 de junio de 2000, FJ: 3 (JT 2000\1779)

El secreto médico también encontró límites con la administración de justicia y de esta forma se empezó a poner más contacto entre la medicina y el derecho, lo que trajo como resultados nuevas disciplinas como la medicina legal/medicina forense. En esta medida, desde hace años ya se exigía a la medicina explicar las conductas delictivas del sujeto, de forma que pudiese comprenderse desde su biología o anatomía las razones de su actuar, al delincuente se le podía considerar un enfermo y al enfermo un posible delincuente. Esta información de la salud es valiosa para el juez, y hasta puede servir de guía, antes de tomar una decisión que afecte las partes en conflicto.

Sobre lo anterior, queremos destacar que la profesión de la medicina pasó de ser una ciencia dedicada exclusivamente a curar a los enfermos, a convertirse en un apoyo fundamental de los tribunales de justicia, ya que, con el análisis de expedientes médicos, se pueden explicar las conductas de algunos delincuentes. Por ejemplo, casos de homicidas en serie, que además de sufrir una enfermedad mental, padecían patologías que condicionaron su actuación ilegal (tumores y malformaciones cerebrales, entre otros).

3.1. ¿Es necesario el secreto médico?

Como ya hemos reiterado, la protección de los datos es un derecho de novedosa vigencia jurídica y el secreto médico se constituye en un medio idóneo, para hacer que este derecho sea respetado por los profesionales en los momentos más difíciles de cada persona. En tales casos, “la observancia del secreto profesional puede ser garantía para la privacidad y el respeto a la intimidad una justificación reforzada para la oponibilidad del secretor de modo que se proteja con éste no sólo un ámbito de reserva y sigilo en el ejercicio de una actividad profesional que, por su propia naturaleza o proyección social se estime merecedora

de tutelar sino que se preserve, también, frente a intromisiones ajenas, la esfera de la personalidad que el art. 18.1 de la Constitución garantiza”⁴³⁴.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE⁴³⁵. Ello adquiere especial relevancia en el caso del secreto médico, habida cuenta de la particularidad de la relación que se establece entre el profesional de la medicina y el paciente, basada firmemente en la confidencialidad y discreción y de los diversos datos relativos a aspectos íntimos de su persona que con ocasión de ella suelen facilitarse. De ahí que el secreto profesional sea concebido en este ámbito como norma deontológica de rigurosa observancia, que encuentra una específica razón de ser no ya en la eficiencia misma de la actividad médica, sino en el respeto y aseguramiento de la intimidad de los pacientes.⁴³⁶

No cabe duda que la historia médica relativa a un paciente es un dato reservado a determinados profesionales que son los que tratan al paciente y no puede ser revelada, salvo autorización judicial⁴³⁷. Sin embargo, ante estas definiciones, cabe aclarar que la cobertura del secreto médico no sólo alcanza la información que el paciente confía al médico, en razón de la profesión, sino todos aquellos signos u otros datos que el profesional observe, antes, durante y después de ejecutar el tratamiento. Por tal motivo, este deber se extiende a todo lo relativo a los resultados de las exploraciones y pruebas practicadas, así como al diagnóstico, pronóstico y a la enfermedad misma y al tratamiento.

⁴³⁴ ATC, 600-1989, de 11 de diciembre de 1989, FJ: 2 (RTC 1989\600 AUTO)

⁴³⁵ SAN, de 1º de diciembre de 2009, FJ: 4 (JUR 2010\35383)

⁴³⁶ SAP de Barcelona, 586-2004, de 13 de diciembre de 2004, FJ: 3 (AC 2005\10)

⁴³⁷ AAP de Madrid, 498-2003, de 18 de junio de 2003, FJ: 1 (JUR 2003\247846)

Aunque también hay que reconocer que, dentro de las debilidades de la naturaleza humana, a veces es difícil separar los roles profesional y humano, siendo esto objeto de crisis en torno a la forma de actuar ante determinado hecho, dando cabida a su vez a la objeción de conciencia⁴³⁸. Por el contrario, la amistad o alta confianza que exista entre médico y paciente, podría dar ocasión a una intromisión en la intimidad familiar del sujeto, bien influenciando mediante su opinión, o bien indagando más allá de lo necesario, con el fin de sacar algún tipo de provecho. Cabe mencionar que el secreto médico no se extingue con la muerte del paciente, siendo obligación del médico mantener en reserva aquella información que pertenezca al enfermo, salvo que exista una obligación legal expresa o estén en juego derechos de terceros. Sobre este tema, el Tribunal Supremo ha señalado que aunque la enfermedad engendra cierto sentimiento de humillación, es algo tan inevitable como comúnmente aceptado, por lo que no se comprende que si esta indeseada contingencia llega a producirse constituya un desdoro que el nombre de una persona figure en la lista de clientes de un médico o de una clínica o institución sanatorial, o el hecho de que esta circunstancia pueda ser conocida por la Administración Tributaria, siempre que sólo se facilite la identificación indispensable y no la historia clínica, el tipo de exploraciones, el diagnóstico, el tratamiento o las intervenciones que puedan orientar sobre la naturaleza del padecimiento o desarreglo que haya motivado la actuación profesional⁴³⁹.

Sobre el particular, esta obligación de secreto parece lógica, pues una sociedad que no atiende a sus ciudadanos enfermos no prospera, siendo imprescindible que los pacientes busquen atención médica a sus problemas de salud, tan pronto fuesen identificados, a fin de garantizar la buena convivencia entre todos. En consecuencia, la confianza entre médico y paciente es fundamental, ya que facilita la pronta intervención ante la enfermedad. Siguiendo ese hilo conductor, el secreto médico era en principio una

⁴³⁸ Entendemos la objeción de conciencia como una negativa, por razones axiológicas, de contenido primordialmente moral, a someterse a una conducta que en principio le sería jurídicamente exigible.

⁴³⁹ STSJ de Asturias, 630-2000, de 5 de junio de 2000, FJ: 3 (JT 2000\1357)

obligación moral, antes de estar tutelada por el ordenamiento jurídico, por eso, en sus inicios el secreto, de los profesionales de la medicina no solo abarcaba el sigilo sobre la información que recibían de los pacientes, sino, también, el secreto del “arte de curar”, el cual no era revelado a cualquier persona, por el contrario sólo se confiaban entre personas con algún vínculo familiar o perteneciente a un selecto grupo, como en el caso de los sacerdotes de Asclepio⁴⁴⁰.

3.2. Fundamento histórico del secreto profesional.

La manifestación del secreto profesional data de principios de la vida en sociedad y está expresado no solo a nivel de “profesiones”, sino en fundamentos contractuales y hasta en las propias religiones. Sus antecedentes podrían ubicarse en Roma, donde existían dos formas de explicar la existencia de este secreto profesional: la “conmiso”, que consistía en la obligación de secreto que se nace de un acuerdo previo a la confidencia, lo cual entre sus efectos tenía transformar lo actuado, en este caso, la confidencia y su correspondiente recibo en una especie de pacto. Asimismo, la “promiso”, que a diferencia de lo anterior, establecía la necesidad de realizar primero la confidencia y, después de recibido, surgía la obligación para el depositario, por el mero hecho de haberla recibido, obviamente con la obligación de no revelarla. También, en el Corpus Juris del Derecho Romano, Digesto⁴⁴¹, se hace referencia a la obligación de no propalar secretos respecto de abogados, procuradores y escribanos.

En la religión católica, por ejemplo, basta analizar el sacramento de la “confesión” para ver como la obligación de silencio o sigillum confessionis se exigía desde tiempos de antaño a los sacerdotes y monjes. Y es que en la iglesia católica se ha dado gran valor el

⁴⁴⁰ En la mitología griega Asclepio o Asclepios (en griego Ασκληπιός), Esculapio para los romanos, fue el Dios de la Medicina y calculación, venerado en Grecia en varios santuarios.

⁴⁴¹ Ley 25 de Test. XXII, V.

secreto y la “virtud” del silencio entre las autoridades eclesiásticas, principios que en ocasiones han jugado un doble rol, plausible en algunos casos y altamente criticable en otros. Los sacerdotes fueron los primeros “médicos” del alma, y como tales recibían de sus fieles diversos tipos de información, las cuales eran merecedoras, en ocasiones, de castigo “moral”, con las correspondientes penas establecidas y aceptadas por la fé.

Ahora bien, en el tema que nos interesa, el secreto médico hunde sus raíces en el juramento hipocrático⁴⁴², en el cual, el nuevo profesional jura que “todo lo que viere u oyere en mi profesión o fuera de ella, lo guardare con sumo sigilo”. Probablemente, y con posterioridad, “el padre de la ética médica haya sido el clínico inglés Thomas Percival en el Londres de los albores del siglo XIX: *Ética Médica*⁴⁴³ (en latín) fueron las dos primeras palabras del larguísimo título de su libro, dedicado a los aspectos éticos del ejercicio de la medicina, con posterioridad, clínicos ingleses de la envergadura de THOMAS SYDENHAM y WILLIAM OSSLER ampliaron los conceptos iniciales y fueron creando un verdadero cuerpo organizado de *Ética Médica* que, en buena parte, reposó sobre este famoso y clásico concepto del secreto médico hoy, desafortunadamente, bastante devaluado”⁴⁴⁴, aunque ya a principios del s. XIX, Jeremy Bentham introduce en occidente el término deontología. Lo hace en el seno del utilitarismo; la deontología nace así: concebida como una suma algebraica que mide la ética en función del análisis coste/beneficio⁴⁴⁵.

⁴⁴² Hipócrates de Cos. Perteneció a la escuela pitagórica, fundada por Pitágoras de Samos, que floreció en Crotona (Sicilia) a fines del siglo V aC.

⁴⁴³ El título completo es *Medical Ethics or a code of Institute and Precepts*, 1803

⁴⁴⁴ WAGNER GRAU, Patrick, El secreto profesional o la discreción del médico (en línea), Simposio de la Academia Nacional de Medicina, año 2006, en http://www.acadnacmedicina.org.pe/publicaciones/Anales_2006/simposio_secreto_profesional_wagner.pdf

⁴⁴⁵ BENTHAM, Jeremy. “Deontology together with a table of springs of action and article on utilitarianism, Edit. Amnon Goldworth, 1983, p. 119

Para GRACIA, es en “los siglos XVIII y XIX en los que el secreto comienza a configurarse como un derecho subjetivo de todo ser humano, si bien se encontraba ya implícito en el siglo XVII, en la relación de los derechos subjetivos y, sobre todo, en el llamado derecho a la libertad de conciencia, entendiéndolo no solo como libertad religiosa o libertad política, sino también como respeto a la intimidad de la persona y no divulgación de los datos que a ella pertenecen”⁴⁴⁶. Este derecho en nuestros días sigue siendo de especial atención para los tribunales de justicia, y aunque está por demás aceptado por los profesionales, no dejan de presentarse las reclamaciones por su violación. De hecho, se sigue perfeccionando en sus modalidades, gracias a la participación de la tecnología en la comisión del delito de revelación de secretos.

3.3. Criterios que le dan fundamento.

Efectivamente, es deber del profesional mantener en estricta confidencialidad lo que se le ha entregado, pero ¿este deber genera un derecho?, Hoy impera la tesis que contempla el secreto bajo un marco de relatividad, garantizando simultáneamente la protección de los datos, la intimidad y otros derechos con los que puede entrar en conflicto, pero ¿se puede hablar del derecho del paciente de exigir al médico su silencio, en cuanto a la información íntima o personal que maneja? Hasta ahora se ha venido hablando del secreto médico como una obligación que vincula al profesional de la medicina, sin insistir demasiado en la contrapartida que ello supone para el paciente. Es decir, en la generación de un derecho para éste al respeto y al mantenimiento del sigilo profesional. La existencia de este derecho parecería, en principio, lógica consecuencia de la obligación de discreción o secreto, pues todo deber tiene como contrapartida el derecho del beneficiario a exigir su cumplimiento. Pese a ello, esta cuestión no es pacífica ni en la doctrina ni en los casos de

⁴⁴⁶ GRACIA, Diego, “La confidencialidad de los datos clínicos”, en CALCEDO O. Alfredo (editor), *Secreto médico y protección de los datos sanitarios en la práctica psiquiátrica*, Madrid, Edit. Médica Panamericana, 2000, p. 23

pronunciamientos jurisprudenciales existentes sobre el particular, en los que se percibe una clara reticencia al reconocimiento del derecho del paciente al secreto médico⁴⁴⁷.

Por un lado, la LGS 14/1986, establece en su art.10.3, que el paciente tiene derecho a la confidencialidad de toda la información relacionada con el proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema. De lo anterior, se infiere que esta garantía debe ser respetada por todas las personas, profesionales o no, que asisten o colaboran en las instituciones, ya que todas ellas tendrían, en mayor o menor grado, una obligación legal, basada en el principio de lealtad hacia el enfermo.

El interés del paciente, es preservar su intimidad y sus datos personales, esto ya está claro, basándose en el derecho fundamental tutelado en el art. 18.1 y 18.4 CE, pues, además de sufrir una enfermedad, esta condición podría generarle consecuencias a nivel social, sobre todo con algunas enfermedades. Por otro lado, está el interés de la comunidad, que es contar con habitantes sanos que estén dispuestos a someterse a un proceso de cura, aunque en el recorrido tengan que compartir parte de su intimidad con los profesionales de la salud. Este interés depende de la verdadera confianza que demuestre el especialista y la verdad que demuestre el paciente. Por último, y no menos importante, está el interés del médico, pues la información que recibe no es pueril en significado, más bien es la base de la cual partirán sus análisis, diagnóstico y tratamiento, de no lograr ese vínculo con el enfermo, mal podría curarle su enfermedad.

En otro orden de ideas, podría decirse que el paciente, mediante el contrato de servicios, acepta como una obligación inminente, la confesión de los verdaderos detalles de sus dolencias, aunque en esa etapa, deba revelar parte de su información personal o su

⁴⁴⁷ DE MIGUEL SÁNCHEZ, Noelia, Secreto médico, confidencialidad e información sanitaria, Edit. Marcial Pons, 2002, pp. 89 y 90

intimidad. En este aspecto, si bien es cierto, el paciente tiene la posibilidad de elegir quién será su médico, esto también implica que sólo puede hacerlo dentro de un grupo determinados de profesionales. En tal sentido, no está en un plano de igualdad, frente a los derechos que posee el médico, sobre todo en los casos de objeción de conciencia, en los que éste último podría elegir si atiende o no a un enfermo.

Es más, de acuerdo a los sistemas de salud que apliquen en su área de residencia, hasta tendría que acogerse a los sistemas que impone un médico de familia, situación que reduce aun más sus opciones de establecer condiciones previas a su atención médica. No obstante, todas las situaciones anteriores no implican una renuncia al derecho a la confidencialidad de la información, de ahí, que se justifica el resguardo de todos los datos que se puedan acumular del enfermo, mientras recibe tratamiento a su condición de salud.

3.4. Bases legales para el secreto médico.

El médico se encuentra obligado, salvo en excepciones muy concretas, a guardar las confidencias que el paciente le hace en el transcurso de dicha relación. La CE de 1978, en su artículo 18.1, no se refiere al secreto profesional, por ende no existe rango constitucional para este “deber de comportamiento”. Aun así, la regulación jurídica del secreto médico en España es abundante y posiblemente dicha pluralidad podrían crear ciertas disquisiciones entre las normas. Las codificaciones médicas y estatales interactúan paralelamente y es evidente que el Código Deontológico no tiene una notable relevancia lo que lleva a que se le tome en cuenta, sobre todo en la elaboración de la jurisprudencia en los Tribunales⁴⁴⁸, siendo casi una herramienta auxiliar, pues impone al personal sanitario deberes de diversa índole. Del mismo modo, y como contrapeso, la codificación estatal también va moldeando las normas deontológicas, siendo éstas más acordes con el derecho positivo vigente.

⁴⁴⁸ SAP de Badajoz, 106-2002, de 16 de mayo de 2002, FJ: 3 (AC 2003\468)

En cuanto a normativa estatal, el secreto médico encuentra fundamento en la LGS 14/1986 que establece, en su art. 10, que “todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias: (...) 3. A la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público”.

De igual forma, el art. 7 de la LOAP 41/2002 proclama el derecho a la intimidad de toda persona y 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, añadiendo que los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes. Asimismo reitera, en los arts. 2.7 y 16.6, el deber de secreto hacia toda persona que elabore o acceda a la información y documentación clínica, así como hacia el personal que acceda a los datos de la historia clínica en el ejercicio de sus funciones.

Más recientemente, el art. 19 de la Ley Orgánica 55/2003, de 16 de diciembre, del Estatuto Marco del Personal Estatutario de los Servicios de Salud establece el deber del personal citado de respetar la intimidad personal de los usuarios, manteniendo la debida reserva y confidencialidad de la información y documentación relativa a los centros sanitarios y a los usuarios obtenida, o a la que tenga acceso en el ejercicio de sus funciones.

Por otro lado, el Código de Ética y Deontología Médica⁴⁴⁹ actual trata el secreto médico en su Capítulo IV, con un total de 4 artículos, contados desde el art. 14 al art. 17. En su redacción reitera que el secreto médico es inherente al ejercicio de la profesión y se establece como un derecho del paciente a salvaguardar su intimidad ante terceros. Todos los

⁴⁴⁹ Aprobado por la Organización Médica Colegial Española, mediante Comisión Central de Deontología, Derecho Médico y Visado, con fecha 10 de septiembre de 1999.

profesionales están obligados a cumplirlo, independientemente de su especialidad, teniendo en cuenta la permanente de reserva de la información, aunque el paciente haya fallecido. Esta obligación es extensible a todos los cooperadores que presten auxilio dentro de la atención sanitaria, siendo cada uno responsable de su preservación, para lo cual, en caso de dudas, deben acudir al colegio en busca de asesoramiento y, por tanto, conocer cuáles son las causas en la que podría levantar dicha obligación al secreto.

3.5. Límites al secreto médico.

El secreto médico siempre ha dejado confusiones, por lo menos en cuanto a su alcance. Ni siquiera el juramento hipocrático escapa a estas dudas, cuando reza que “callaré todo lo que pueda ver y oír referido a los seres humanos que no tenga necesidad de ser divulgado”. La duda salta a la vista, ¿qué tiene y qué no tiene la necesidad de ser divulgado?, ¿quién lo determina?, ¿acaso es potestad del médico? o ¿puede ser determinado por el propio paciente? En este sentido, aunque el médico pudiese determinar qué debe ser confidencial, tal condición no lo autoriza a divulgar a otras personas la información íntima que posee del paciente. Esta prohibición alcanza inclusive a sus familiares más cercanos, por lo que es inaceptable que se intente justificar la revelación de la información clínica a personas de alta confianza del galeno. Tal conducta ya fue analizada cuando se sancionó a un médico⁴⁵⁰ por permitir que su esposa, hija y colega de “otra especialidad”, completaran sus formularios y prescripciones hospitalarias, para lo cual accedían libremente y sin reparo, a los expedientes de los pacientes. Lo planteado por el médico, en defensa a su comportamiento no fue admitido por el tribunal. De igual forma, la incógnita subsiste, pues es evidente que no es igual el nivel de sigilo que se debe tener en cuanto a una enfermedad mental o una enfermedad venérea, como para aquellos casos en los que se aplica una simple sutura de una herida.

⁴⁵⁰ STSJ de Galicia, 438-1999, de 5 de mayo de 1999, FJ: 3 (RJCA 1999\1545)

Si bien existen enfermedades de obligatoria comunicación al Estado y, ni el médico, ni el paciente, tienen la posibilidad de negarse a informar lo pertinente en estos casos. Más difícil sigue siendo determinar los niveles de responsabilidad que quedan en torno al conocimiento y resguardo de los datos, ya que hoy vivimos un contexto mucho más despersonalizado, en el que a la par del crecimiento de la medicina hospitalaria, en razón de mayores conocimientos científicos, es más común trabajar en equipo y en el marco de una asistencia plural de especialistas, en los que los datos recibidos del enfermo se recopilan de forma más o menos mecánica, por lo que a ellos pueden acceder, no sólo cualquier sanitario del centro, sino personal administrativo, subalternos, o incluso cualquier usuario de la red interna administrativa. Siguiendo a MORALES PRATS, las personas que se ven en la necesidad de acudir a la obtención de servicios proporcionados por determinados profesionales ven limitadas por las circunstancias la preservación de su intimidad. En esa limitación, traducida en accesibilidad a la vida privada ajena, radica el fundamento del secreto profesional, que ostenta el rango de deber jurídico, más allá del deber ético/profesional⁴⁵¹.

Conviene entonces anotar que no se trata de un privilegio o una patente de curso, aunque si existen algunas modalidades al secreto médico. Por un lado, existe un secreto médico compartido cuyo fundamento se encuentra precisamente en la atención en equipo que se brinda al paciente, especialmente cuando para llegar a un diagnóstico, pronóstico o tratamiento adecuado se requiera la participación de distintas especialidades en el área de salud (personal de enfermería, laboratorio, farmacia, auxiliares, celadores, estudiantes en prácticas de medicina o enfermería, etc.). Lo importante a destacar es que cada uno de los profesionales que intervine en la cadena de servicio tienen también la obligación de mantener el secreto, por pertenecer al mismo ámbito de atención sanitaria, siendo difícil que la información se comparta con alguien que no reúna esas características principales. Del mismo modo, tal como hemos insistido en líneas y capítulos anteriores, la elaboración y manejo de las historias clínicas implican la participación de personal no

⁴⁵¹ MORALES PRATS, Fermín, Op. Cit., p. 441

necesariamente médico, por lo que bien podría considerarse la existencia de un secreto médico derivado, en especial por el personal administrativo, en lo que se puede incluir los del propio hospital o centro de atención, como otros incidentales (personal de justicia o compañías aseguradoras, etc.).

3.6. Excepciones al secreto médico.

En principio, el secreto médico debe preservarse por encima de cualquiera intervención de otras personas, sin embargo, toda norma tiene su excepción, y en este caso, operan varios supuestos en los que no resulta de aplicación esta exigencia: consentimiento del paciente, la autorización de la ley, la declaración de enfermedades, el registro de nacimientos y defunción, revelar el secreto a favor del paciente o de un tercero o revelar la información en favor del propio médico.

3.6.1. Consentimiento del paciente.

El secreto médico puede ser levantado por autorización del propio paciente, quien al otorgar el consentimiento puede liberar al médico del deber de sigilo sobre la información que posee, el consentimiento puede ser expreso o tácito según las condiciones de cada caso. Sin embargo tal posibilidad no debe comprometer la relación o nivel de confianza existente entre profesional y paciente.

En principio, toda revelación que se haga prescindiendo del consentimiento del afectado ha de respetar escrupulosamente el principio de reserva de ley bajo criterios de excepcionalidad, por eso el Código Deontológico de 1999, lo contempla con esa modalidad, producto de la voluntad del paciente. Y es que, como señala GOMEZ RIVERO, el enfermo es, ante todo, un sujeto pleno de derechos, entre los cuales se encuentra el del respeto de su voluntad e intimidad y, con ellos, de su propia dignidad, que no son más que plasmaciones en

este ámbito del reconocimiento de otros tantos derechos que a nivel general le competen, ya antes que como enfermo, como persona, asimismo, más allá de esta exigencia básica, el consentimiento, para ser eficaz, ha de prestarse en un momento temporal que garantice la madurez de la decisión⁴⁵². No obstante, esta autorización no puede conllevar un perjuicio para el médico, ya que en algunos casos el paciente puede sacar ventajas en cuanto al contenido del secreto, permitiendo su uso en aquellos supuestos en los que tenga un interés determinado como, por ejemplo, la confesión de un delito mientras recibe atención médica.

Lo más importante en este caso, según nuestro criterio, es no perder de vista que el paciente es el único titular de su intimidad, y tal como lo expresamos en el capítulo anterior, es quien determina qué se mantiene dentro de su esfera interior y qué quiere compartir con el resto de la sociedad. Tanto la intimidad como el honor pueden verse afectados con la liberación de la información, especialmente si son datos de salud. Aunque, como señala VIVES ANTON, finalmente el consentimiento del ofendido puede también justificar la lesión del honor, al ser éste un bien jurídico esencialmente disponible. Procede hablar, en tal caso, de justificación y no de atipicidad, sobre todo si se define el honor como correlato de la dignidad humana⁴⁵³.

Sobre el particular, el paciente no puede alegar que existe violación del secreto médico si la comunicación a un tercero ha sido previamente autorizada⁴⁵⁴, con lo cual el médico simplemente se comporta dentro de los términos y autorizaciones que se le han concedido. En esencia, el consentimiento del titular del secreto dará lugar a la exclusión del

⁴⁵² GOMEZ RIVERO, María del Carmen, La responsabilidad penal del médico, Edit. Tirant lo blanch, Valencia, 2003, p. 67

⁴⁵³ VIVES ANTÓN, Tomás, Op. Cit., p. 320.

⁴⁵⁴ AAP de Barcelona, de 24 de enero de 2000, FJ: 1 (ARP 2000\958)

injusto penal⁴⁵⁵, por lo que sería incongruente alegar que el médico no ha cumplido su labor, si previamente se les ha permitido la comunicación a personas distintas al paciente.

Cabe en este tema analizar el concepto de las certificaciones de salud, en las que el médico, a solicitud del propio paciente, debe extender una constancia que describa las condiciones de salud de la persona. Efectivamente, se están exponiendo a terceros elementos que podrían considerarse como íntimos de la persona, pero sólo se logra con base a una autorización previa y tácita del paciente y tal como señala REBOLLO VARGAS, al mediar el consentimiento por parte del cliente, propiamente no cabrá hablar ya de secreto⁴⁵⁶.

De igual forma, se debe tener en cuenta la capacidad para otorgar el consentimiento, haciendo referencia a las características ya mencionadas en páginas anteriores, que establece la LOAP 41/2002, sobre los menores de edad emancipados o no y las personas que sufren alguna discapacidad.

De esta manera, la persona/ paciente puede disponer libremente de sus datos y, por ende, de su intimidad, y despojarse voluntariamente de la protección establecida por la ley. Esta característica, según GONZÁLEZ RUS, supone una diferencia fundamental con otros bienes jurídicos penalmente protegidos, a diferencia de lo que sucede, por ejemplo, con la vida, la salud, la libertad sexual, etc., que aun siendo disponibles por el sujeto, tienen un contenido sustancial que no depende de la voluntad del titular, sino que viene impuesto por un sustrato ideal o material predefinido por las características objetivas del bien y semejante en todos los casos. El bien jurídico intimidad, por ejemplo, tiene un sustento exclusivamente subjetivo, puesto que depende de la voluntad de cada sujeto y varía en cada sujeto, lo que

⁴⁵⁵ CÓRDOBA RODA, Juan, Abogacía, secreto profesional y blanqueo de capitales, Edit. Marcial Pons, Madrid/Barcelona, 2006, p. 32

⁴⁵⁶ REBOLLO VARGAS, Rafael, La revelación de secretos e informaciones por funcionario público, Barcelona, 1996, p. 181

coloca a ésta en el centro de la noción de intimidad, por ser la que define el contenido sustancial del bien y el ámbito de protección penal⁴⁵⁷.

Ahora bien, es importante destacar que GARCÍA HERNÁNDEZ aclara este aspecto y dice que sin perjuicio de lo anterior, no hay que olvidar que, en ocasiones, la historia clínica recoge datos relativos a terceras personas distintas del propio paciente. Por ello, en tales casos, no bastará con la autorización explícita del mismo, sino que además deberá recabarse el permiso de los terceros implicados. En este mismo sentido, la autorización judicial para el acceso a los datos clínicos deberá también referirse al levantamiento de la privacidad (intimidad), de ese tercero y no solo del propio paciente⁴⁵⁸.

3.6.2. Autorización de la ley.

En estos casos el médico se someterá a los parámetros establecidos por la norma y deberá “cooperar” con la autoridad cuando le sea requerido. Este tema puede generar diversas interpretaciones, algunas muy comprometedoras con la profesión de la medicina y en consecuencia con aquel pilar de la “confianza” que debe existir dentro de la profesión sanitaria. El ser llamado ante la autoridad para revelar información íntima del paciente presenta, como casi siempre, un tema de conflicto y de ponderación entre intereses. En este caso, el interés de la prueba procesal, consistente en la búsqueda de la verdad material, que utiliza como instrumento la obligación de denunciar y de declarar, y, de otro lado, el derecho /deber de silencio que impone el secreto profesional⁴⁵⁹. MUÑOZ CONDE señala que, en principio, el médico puede negarse a actuar como perito en un juicio en relación con el

⁴⁵⁷ GONZÁLEZ RUS, Juan, Op. cit., p. 324

⁴⁵⁸ GARCÍA HERNÁNDEZ, Tomás, Manual del médico clínico para evitar demandas judiciales, Op. Cit., p. 87

⁴⁵⁹ MICHAVILLA NÚÑEZ, José, “El derecho al secreto profesional y el artículo 24 de la Constitución. Una visión unitaria de la institución”, en Estudios sobre la Constitución Española, Tomo II; Edit. Civitas, Madrid, 1991, p.1431

estado mental de un paciente si su testimonio puede servir como prueba para incriminarlo o para eximirle de responsabilidad, salvo que éste lo autorice a ello; y negarse a suministrar los datos que haya obtenido en su relación profesional con el paciente; por ello no puede llevarse hasta las últimas consecuencias en caso de que esté en peligro de la vida o los derechos fundamentales de otra persona⁴⁶⁰.

Lo primero en destacar, es el rol del médico ante la autoridad, y la necesidad inexcusable de develar la información calificada como secreto, para lograr descifrar la responsabilidad dentro de un caso determinado. Ya la Ley de Enjuiciamiento Criminal señala, en su art. 410, que todos los que residan en territorio español, nacionales o extranjeros, que no estén impedidos, tendrán obligación de concurrir al llamamiento judicial para declarar cuanto supieren sobre lo que les fuere preguntado si para ello se les cita con las formalidades prescritas en la ley. A esto se le suma el hecho de que, si el médico en el ejercicio de su profesión tiene conocimiento de la comisión de algún delito, o tiene fuertes indicios de que en un futuro próximo uno de sus pacientes puede cometer algún delito, tiene que comunicarlo ante la autoridad policial, so pena de sanción, tal como establece el art. 262, de LEcrim cuando señala que los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio Fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio, si se tratare de un delito flagrante. Este artículo hace especial referencia al profesor en medicina, cirugía o farmacia, destacando la gravedad en caso de que quien omite se especialista de estas “profesiones”. Sobre el particular, señala GARCÍA HERNÁNDEZ que desde distintos auditorios, médicos, letrados, incluso algún magistrado, han manifestado que el médico puede plantear objeciones para no entregar la historia clínica al juez, en la medida que pueda contener datos íntimos de su paciente, como hijos no esperados, procesos de separación y divorcio, herencia o de terceros cuyas

⁴⁶⁰ MUÑOZ CONDE, F., Op. cit., p. 268

anotaciones no sean necesarias para el juicio y quiebra el deber del secreto profesional⁴⁶¹. Sin embargo, en cuanto a estas objeciones, no compartimos tan autorizada opinión, pues consideramos que un juez debe recibir toda la información que existe en el dossier médico, pues igualmente tiene la obligación de mantener en reserva lo que el médico le confía, sobre todo si esta información le permite conocer la realidad vivida por el paciente y, en consecuencia, tomar las decisiones de rigor.

Entendemos que dentro de esta obligación se incluyan imperativamente a los médicos, salvo que ejerzan como funcionarios públicos. Sin embargo, nos llama la atención, y por eso lo veremos más adelante, que esta misma ley, a diferencia del profesional sanitario, si excluye taxativamente a otras profesiones, como la del derecho, pues el artículo 263 de la LEcrim, señala que la obligación impuesta en el párrafo primero artículo anterior “no comprenderá a los Abogados ni a los Procuradores respecto de las instrucciones o explicaciones que recibieren de sus clientes”.

Lo realmente criticable en este aspecto es el rol que desempeña el médico en estos casos. Parece más una extensión del poder judicial que un profesional encargado de la salud de las personas. Este cambio produce severas críticas en cuanto al nivel de correspondencia y certeza que puede tener el paciente ante la profesión médica. En sí, el testimonio del médico, generalmente mediante informes o declaración verbal, puede brindar la certeza⁴⁶² que requiere lo alegado por algunas de las partes dentro del proceso, lo que evidentemente consistiría en la liberación del secreto a favor de uno y en contra de otro.

Y es que podría producirse un caso de “estado de necesidad”, conforme el art. 20.5. del Código Penal Español, como eximente de responsabilidad criminal. Nosotros coincidimos en que dichas “dudas” sobre el alcance de la protección al secreto profesional, y

⁴⁶¹ GARCÍA HERNÁNDEZ, Tomás, Manual del médico clínico para evitar demandas judiciales, Op. Cit., p. 95

⁴⁶² SAP de Santa Cruz de Tenerife, 1322-2004, de 29 de octubre de 2004, FJ: 1 (JUR 2004\302195)

en nuestro caso el secreto médico, pueden ser resueltas de una mejor forma si se desarrolla con mayor profundidad el derecho establecido en el art. 24. 2 de la CE. En este sentido, aun persiste el debate si es necesario pasar de un "principio", que en ocasiones es más de intención que de ejecución, a una "regla", con carácter más programático y que puede definir los derechos de las partes y, sobre todo, el alcance o vigencia que tiene para el profesional, la protección de la información que posee de su cliente/paciente.

Este tema lo aborda el profesor LAPORTA, cuando señala que la incerteza jurídica es sencillamente no poder saber con precisión lo que jurídicamente se es, es decir, no poder saber qué sujeto de derecho se es, no poder conocer el alcance del propio estatus en una relación dada, o no poder determinar el contenido y los límites de los propios derechos y deberes⁴⁶³. Claro está, entendemos que habrá situaciones en las que una interpretación cambiaría el sentido de la regla, pero establecer múltiples códigos deontológicos de acuerdo a cada profesión, sin llegar al desarrollo de una norma general o estatal, provoca lagunas o conflictos entre normas, que después requieren, en última instancia, el apoyo del poder judicial para poder resolver las dudas en torno a la aplicación del Derecho. Precisamente, una interpretación literal del artículo 24.2 de la CE nos llevaría a pensar que sólo los secretos familiares y profesionales estarían reconocidos como obstáculos admisibles a la adquisición de medios de prueba⁴⁶⁴. Sin embargo, el hecho de dejar la regulación pendiente de mayor desarrollo, podría amparar, en ocasiones, diferentes interpretaciones en este aspecto.

Ahora bien, sobre este tema, la Constitución Española nos presenta dos artículos de notable interés. Por un lado, está el artículo 20.1 d. y, por el otro, el artículo 24.2. Ambos

⁴⁶³LAPORTA, Francisco, "Certeza y predecibilidad de las relaciones jurídicas", en LAPORTA, F, RUIZ MANERO, J, RODILLA, M, Certeza y predecibilidad de las relaciones jurídicas, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 56

⁴⁶⁴OTERO GONZÁLEZ, M^a del Pilar, La Revelación del secreto de estado, en los procedimientos penales, Edit. Tirant lo Blanch, Valencia 2000, p .22

se refieren al secreto profesional que debe regularse, pero desde fines y bienes jurídicos totalmente diferentes. Siendo así, coincidimos con FRIGOLA VALLINA Y ESCUDERO MORATALLA, cuando señalan que, en el primero de los supuestos, se refiere al secreto profesional del periodista, cuyo fondo no busca proteger la información que posee, la cual trata de develar evidentemente, sino la fuente de la cual ha tomado los datos (libertad de expresión). A sensu contrario, el artículo 24.2, se refiere al secreto profesional de otros especialistas, como el abogado o el médico, que sí requieren mantener en reserva la información que poseen, aunque se conozca la identidad de su titular (derecho a la intimidad)⁴⁶⁵.

3.6.3. La declaración de enfermedades.

Esta excepción está fundamentada en el principio de la protección general de la sociedad, y busca evitar que enfermedades contagiosas se propaguen sin control entre los integrantes de la comunidad. Obviamente, las epidemias son uno de los problemas más apremiantes para una sociedad que busca la salud y dado que los médicos son los primeros en estar en contacto con las personas que presentan signo de enfermedad, están en la obligación de informar si existen amenazas que pudiesen interrumpir la tranquilidad de las personas. De este modo, es el personal médico el que está obligado a declarar los casos de nuevos diagnósticos de infección a través del formulario de notificación contenido en el Anexo I del Real Decreto 2210/1995. Y ese régimen peculiar se ahonda en el ámbito de la vigilancia epidemiológica, precisamente por la naturaleza de las enfermedades de que se trata, en cuyo sentido el art. 33 del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica, establece la declaración obligatoria de

⁴⁶⁵ FRIGOLA VALLINA, Joaquín y ESCUDERO MORATALLA, José, Honor, secreto profesional y cláusulas de conciencia en los medios de comunicación. Límites y aspectos jurídicos civiles y penales, Ediciones Revista General de Derecho, Valencia, 1998, pp. 87 y 88

estas patologías, una vez detectadas por el profesional correspondiente (...) ⁴⁶⁶. En tal sentido, los médicos no están obligados a informar previamente al paciente que se dará cumplimiento a lo establecido por la norma, en cuanto a la notificación y registro correspondiente de la enfermedad.

En este orden de ideas, la Ley Orgánica 3/1986 sobre medidas especiales de salud establece, en su artículo 2, que las autoridades sanitarias competentes podrán 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 que se desarrolle una actividad. Para lo que la LGS 14/1986 en su art. 18.13, comisiona a las Administraciones Públicas, a través de sus servicios de salud y de los órganos competentes, para que realicen la difusión de la información epidemiológica general y específica para fomentar el conocimiento detallado de los problemas de salud. Todo esto se hace, de acuerdo a la LOAP 41/2002, art. 6, que dice que 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. Y dice en su artículo 9, que cuando existe riesgo para la salud pública a causa de razones sanitarias, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán a la autoridad judicial en el plazo máximo de 24 horas siempre, que dispongan el internamiento obligatorio de personas.

Con miras a establecer una guía sobre los procedimientos y enfermedades de obligatoria denuncia, se aprobó el Real Decreto 2210/1995, en cuyo texto se desarrolla el procedimiento de denuncia que debe ser seguido, en caso de identificar alguna enfermedad

⁴⁶⁶ STSJ de Galicia, 5-2008, de 16 de enero de 2008, FJ: 4 (RJCA 2008\700)

contagiosa, tanto a nivel de la comunidad autónoma, como a nivel nacional. Llama la atención en este Real Decreto que incluye un Anexo, con 33 enfermedades contagiosas, entre las cuales se mencionan: botulismo, brucelosis, cólera, difteria, disentería, enfermedad meningocócica, fiebre amarilla, fiebre tifoidea y paratifoidea, entre otras. El síndrome de inmunodeficiencia adquirida (SIDA), es de las enfermedades que ostentan la mayor prioridad en su denuncia, siendo desarrollado su manejo en un capítulo especial dentro del Real Decreto 2210/1995.

3.6.4. El registro de nacimientos y defunción.

Otro de los momentos en los que se podría interpretar como propio de revelación del secreto médico, es la inscripción en el Registro Civil. No en todos los casos, efectivamente, sino en aquellos en los que se tenga que identificar si hubo problemas con el nacimiento, con resultado de muerte, o si ésta consecuencia está acompañada de algún padecimiento o enfermedad, sobre todo si la misma puede causar “amenaza” a la comunidad y, del mismo modo, en los casos de defunción en las que pudiesen existir enfermedades, que en antaño fueron catalogadas como “deshonrosas”, en caso de la que las mismas puedan ser contagiosas y de peligro. Y es evidente que no se consideran con carácter general intromisiones ilegítimas las actuaciones autorizadas o acordadas por la autoridad competente de acuerdo con la ley. Entiéndase que la ley solo puede autorizar esas intromisiones por “imperativos de interés público”.⁴⁶⁷

3.6.5. Revelar el secreto a favor del paciente o de un tercero.

Mantener el secreto del paciente depende mucho de la capacidad que éste tenga o demuestre durante el proceso de atención en la instancia de salud. En los casos de

⁴⁶⁷ SJP de Palma de Mallorca, 71-2001, de 14 de marzo de 2001, FJ: 4 (JUR 2001\118392)

menores de edad⁴⁶⁸ o personas con discapacidad mental que no entiendan las consecuencias de su tratamiento, existen criterios especiales. Efectivamente, en estos casos requieren de una representación que recaerá usualmente en sus padres o tutores, a quienes es posible descubrir la información del padecimiento que sufre el hijo, tomando en consideración los criterios establecidos por la LOAP 41/2002, sobre la de autonomía del paciente.

La LOAP 41/2002, en su art. 5. 3, establece que cuando el paciente, según el criterio del médico que le asiste, carezca de capacidad para entender la información a causa de su estado físico o psíquico, la información se pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho. Asimismo, con las actuales enfermedades contagiosas, tipo sífilis o SIDA, se ha discutido si existe el derecho de descubrir el secreto en aquellos casos en los que el enfermo no desee comunicar a su pareja el padecimiento de dicha enfermedad mortal. De permitirse una libre disposición sobre este tema, entraría en juego la propia vida de un tercero, que en ningún momento aceptaría que se le arriesgara sin el derecho a decidir si está dispuesto/a soportar las posibles consecuencias.

En estos casos, podría el médico revelar la información que posee en cuanto a la condición médica del paciente. Con esta comunicación no está actuando de forma ilícita, sino cumpliendo una obligación deontológica⁴⁶⁹, tomando en consideración la ponderación de derechos que mencionamos en el capítulo anterior. En esto, reiteramos que el derecho fundamental a la protección de los datos y a la intimidad del paciente encuentran sus límites en los derechos de terceros, siendo la vida del compañero/a, un bien jurídico a proteger, tal como se valoran en los casos de estados de necesidad.

⁴⁶⁸ Aclaremos que cuando se trate de menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, pueden hacer uso de su propia información y tomar libremente su decisión. Sin embargo, en caso de actuación de grave riesgo, según el criterio del facultativo, los padres serán informados y su opinión será tomada en cuenta para la toma de la decisión correspondiente.

⁴⁶⁹ AAP de Álava, 268-2005, de 28 de noviembre de 2005, FJ: 1 (JUR 2006\13105)

No en vano tendríamos que mencionar también el estado de indefensión en el que se colocaría a la ciudadanía, teniendo en consideración que habría mayor porcentaje de exposición a un contagio, lo que representa un mayor número de enfermos y un desgaste más significativo para la sanidad y los recursos que esto conllevaría. Ahora bien, la sola publicidad de la condición médica del enfermo, sin las reservas del dato anónimo, conlleva al paciente una difícil consecuencia, que es ser “expuesto” ante la comunidad por su enfermedad, con el correspondiente rechazo y discriminación.

3.6.6. Revelación en favor del propio médico.

La función de médico no implica la de ser un héroe. Por ende, como cualquier otra persona, tiene derecho a proteger sus intereses, cuando los mismos sean puestos en riesgo, por un actuar poco “loable” del propio paciente. En estos casos, el médico pasa a ser la víctima de su paciente que, en ocasiones y con segundas intenciones, cambia algunas realidades en el proceso de atención, con el fin de confundir y obtener otros beneficios. Siendo así, el médico podría revelar parte del secreto que se le ha confiado, pero sólo en aquellos datos que se relacionen estrictamente con la realidad de lo actuado y aclarar su participación y buen nombre.

Por otro lado, existen los casos donde el médico reclame el pago de sus honorarios, los cuales no han sido honrados por el paciente. En estos casos debe señalar los procedimientos y técnicas médicas aplicadas, tratando de salvaguardar las descripciones exactas de la patología que padece el paciente. Ahora bien, si para justificar su cobro, se ve en la obligación de señalar más datos del tratamiento, entonces deberá ajustarse a todo lo que supiere, para no incurrir en el falso cobro de honorarios, con las correspondientes sanciones por tal comportamiento que va en contra de las disposiciones legales.

De igual forma, la ponderación que se tenga en estos supuestos cobra extrema importancia, ya que están en juego el beneficio del paciente o la protección de los derechos del médico. La decisión de revelar dichos datos confidenciales puede afectar la relación profesional que existe entre médico y enfermo, por tanto, si al médico no le queda otra alternativa, deberá revelar la información con las máximas restricciones posibles y procurando el menor perjuicio para el paciente.

3.7. El secreto y el médico de la empresa.

Luego de múltiples conquistas laborales, se aprobó como una obligación principal de los patronos, permitir a sus trabajadores ausentarse de la empresa en horas laborales para recibir atención médica en los hospitales y clínicas siempre que por sus condiciones de salud o laborales lo requirieran. Esta situación, ocasionaba en los patronos pérdidas cuantiosas por el tiempo que el empleado dejaba de laborar, sobre todo si toma en cuenta que al mes, varios trabajadores pueden solicitar los mismos beneficios, es una suma cuantiosa en dinero, por lo que se convertía en un problema de carácter económico para las empresas.

Por esta razón, se estableció la figura del médico de empresa, como una alternativa que reduce la salida de personal de la institución, baja los costos por el tiempo pagado y no laborado, permite al patrono cumplir con sus objetivos de producción, ventas e ingresos.

Sobre el particular, surgen dudas si realmente puede garantizarse la confidencialidad de los datos que maneja este tipo de médicos con sus pacientes. Y es que, en todo caso, el dictamen del médico puede determinar la continuidad laboral de los trabajadores, pues de no cumplir con las condiciones básicas para el desarrollo de las funciones, basta con la elaboración del informe para que sea cesado en sus labores. La incertidumbre surge por las obligaciones que tiene el médico con el empleador, quien en todo caso es quien contrata al galeno. Aunque esto es así, somos del criterio que entre el

trabajador y el médico debe existir la misma confianza que preside la relación médico-paciente y ello exige la garantía de confidencialidad del médico, sobre todo aquello que conozca del trabajador, sobre todo por garantizar la confianza necesaria.

Ahora bien, en este sentido también hay reconocer que existen límites al derecho del trabajador, especialmente si de su condición de salud dependa su propia seguridad o la de terceros, pues si ésta corre riesgo, no se puede argumentar la obligatoriedad del secreto. Sobre el particular, ya la Audiencia Provincial ha resuelto, por ejemplo, en un caso sobre un conductor de autobús, en los que señala que no existe delito para el médico por revelar la información del paciente, pues se limita a comunicar y dar cuenta a la autoridad administrativa competente, del resultado del reconocimiento médico anual evaluado por el servicio médico de prevención (...). No se habla ni menciona en la comunicación enfermedad alguna, incluso, en el certificado de aptitud, como chófer de autobús se señala que se está pendiente de informe de especialista. Pues bien, si la comunicación no contiene dato preciso que afecte ni vulnere la intimidad del denunciante, es claro que se impone el sobreseimiento....⁴⁷⁰ De igual forma, también se analiza si dentro de la información de salud también se tendrá que informar sobre los resultados de un análisis genético que revelen la predisposición del trabajador a padecer una enfermedad grave de origen genético posterior a ser contratado.

Sobre lo anterior, hemos mencionado en este trabajo que, aunque genéticamente exista predisposición para una enfermedad, no existe certeza completa de que tal enfermedad se presente en el futuro próximo del empleado.

3.8. El secreto y el médico forense.

La medicina forense es una parte de la medicina que determina el origen de las lesiones o muerte de una persona mediante el examen de su cuerpo o cadáver. A través de

⁴⁷⁰ AAP de Sevilla, 162-2006, de 18 de abril de 2006, FJ: 2 (JUR 2006\262638)

esta especialidad se aplican las ciencias médicas a la ilustración de los hechos investigados por la justicia. De igual forma, sirve para el asesoramiento, perfeccionamiento y evolución de las leyes y tiene un profundo compromiso con valores ético deontológico, básico del ejercicio profesional.

Los profesionales que ejercen esta rama de la medicina son los médicos forenses, los cuales regularmente son empleados de los tribunales, para determinar mediante informes, las asesorías y las guías que requieren las autoridades de justicia.

Esta profesión también surge por la necesidad de conocimientos clínicos y biológicos para resolver algunos delitos, que de otra manera no podrían resolverse, por lo que su propósito no es curar a los enfermos, sino establecer premisas que puedan solucionar dichos problemas en términos técnicos que sean comprensibles para los juzgadores.

La figura del médico forense también trae aparejada cierta dificultad con el deber del secreto médico, pues se expone al conflicto entre la obligación de informar al tribunal sobre una causa en específico y su correlativo deber de secreto. Evidentemente, si está compelido por la autoridad no tendría más remedio que informar, sobre todo si su labor es precisamente la de asesor del tribunal. Esta obligación no entraría en conflicto con el artículo 417 del Código Penal, que prohíbe a los funcionarios al servicio de la Administración de Justicia revelar información declaradas secretas.

3.9. Diferencias entre el secreto profesional del médico y el secreto del abogado.

A diferencia de los médicos, el secreto profesional es bastión de la independencia de los abogados y les exime tanto de la obligación de denunciar los hechos que conozcan como consecuencia de las explicaciones de sus clientes (art. 263 de la LEcrim), como de testificar sobre aquellos hechos que el imputado haya confiado a su Letrado en calidad de

defensor (art. 416.2. de la LEcrim). Sólo así el cliente puede hablar con libertad y con confianza con su abogado, contándole, narrándole todos los hechos, sean o no delictivos, de tal forma que el abogado con todos los datos en la mano, pueda plantear de la forma más conveniente la estrategia procesal que crea más conveniente para la defensa de su cliente. Si el cliente no pudiera facilitar a su abogado toda la información de que dispone, ni poner en su conocimiento todos los hechos por temor a que alguno de ellos pudiera ser utilizado en su contra, creemos que no se ejercería el derecho de defensa con la extensión, profundidad y plenitud que desea el legislador constitucional cuando dice en el art. 24 que “todos tienen derecho... a la defensa”⁴⁷¹.

Igualmente, el artículo 416.2. de la LEcrim, dice que el Abogado del procesado respecto a los hechos que éste le hubiese confiado en su calidad de defensor, está dispensado de la obligación de declarar. Esta clara diferenciación denota cierto “privilegio”, que no es reconocido como tal, por las profesiones excluidas, aunque si marca un criterio de “diferenciación”, a favor de unos y contra otros.

Para SÁNCHEZ STEWART, el secreto se justifica en el caso del asesoramiento en el derecho del cliente a su intimidad, derecho fundamental consagrado por la Constitución y como deber genérico es consustancial con la abogacía. Esta no existiría sin ese principio, que nunca debe ser entendido como un privilegio que beneficia al abogado⁴⁷². Tampoco comprenderá a los eclesiásticos y ministros de cultos disidentes respecto de las noticias que se les hubieren revelado en el ejercicio de las funciones de su ministerio.

⁴⁷¹ SAP de las Palmas, 147-2001, de 12 de noviembre de 2001, FJ: 4 (ARP 2001\881)

⁴⁷² SÁNCHEZ STEWART, Nielson, “Aún quedan trincheras (algo sobre el secreto profesional y a prevención del blanqueo de capitales”, en Revista Miramar, Revista del Ilustre Colegio de Abogados de Málaga, Noviembre/diciembre, 2007, número 168, p. 9

DE TOLETO y UBIETO⁴⁷³, señalan que esta desproporción en cuanto al secreto médico, por ejemplo, se debe a que existen otros elementos que hacen relativo su afectación ante los tribunales. Según estos autores, con esta desproporción se pretende evitar que el médico obtenga provecho o beneficios por su silencio. Asimismo, es un tema meramente práctico, pues los jueces también se auxilian con otros médicos que bien pueden aportar información, desde dicha especialidad, al buen desarrollo del proceso y por último, tal actuación representa una verdadera ayuda a la justicia, y como es deber de todos cooperar en su búsqueda, la ponderación de ambos criterios inclinan la balanza a favor de la liberación del secreto. En esto último señalan que la participación del médico podría darse desde la etapa sumarial del proceso, la cual es reservada por naturaleza⁴⁷⁴ y que, en el caso de que en la fase oral se tenga que hacer alusión a dichos datos, el juez está facultado para disponer que la sesión se realice a puerta cerrada, preservando en todo momento la intimidad propia del paciente.

3.10. La revelación de secretos en el Código Penal español, artículo 199.

Dado que nuestro trabajo involucra la protección de los datos y en especial la atención que dispensa el personal sanitario a los enfermos, en el uso de sus datos de salud,

⁴⁷³ DE TOLEDO Y UBIETO, Emilio, Algunas reflexiones sobre el tratamiento jurídico del secreto profesional, en Revista La Ley, volumen 1, 1983, p. 1137 - 1139

⁴⁷⁴ El secreto sumarial alcanza al contenido de los actos de investigación tendentes a la comprobación del delito (inspección ocular, recogida de muestras o vestigios, autopsia), a la averiguación e identificación de la persona a la que se atribuya el hecho punible y a la de sus circunstancias personales (reconocimientos de identidad, reconocimientos médicos y al aseguramiento de los medios materiales que puedan servir para su prueba en el acto del juicio (recogida y conservación de piezas de convicción), así como al contenido de las declaraciones de los imputados y de los testigos documentadas en las actuaciones, a los informes periciales, ya individuales ya de colegios o corporaciones, y a los documentos que se incorporan a la causa, entendiéndose por tales los elementos consistentes en la representación o reproducción de un suceso o narración contenidas en cualquier soporte, que pueden contribuir a la comprobación del hecho y al descubrimiento de su autor.

hacemos una especial referencia al artículo 199 del Código Penal, pues describe en sus dos apartados los ámbitos en los que se puede violar el secreto de la información médica. En ambos apartados, aunque presentan elementos comunes, se diferencian, en virtud de la clase de actividad que desarrolla el sujeto activo, según se derive ésta de una relación laboral o de una actividad profesional. Como anotación general, debemos señalar que la cobertura penal del secreto profesional en general es todavía insuficiente. No obstante, si bien la regulación referida resulta muy novedosa desde la perspectiva del Código Penal de 1973, al que vino a sustituir, no lo fue tanto respecto al proyecto de 1994 que le precedía. Así, si bien se mantiene la tipificación de los delitos contra la intimidad y familiar en un mismo título y además separado de los atentados contra el honor, cambia la rúbrica tanto del título como del capítulo en que se insertan⁴⁷⁵.

Sobre el particular, el artículo 199 del Código Penal español, establece en el primer apartado que “el que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses” (la cursiva es nuestra). En este apartado se pueden incluir primordialmente a los funcionarios y trabajadores sanitarios que cumplen tareas de apoyo en los centros asistenciales, dado su vínculo laboral y la facilidad en conocer la información catalogada como privada. Esta colaboración no requiere, en ocasiones, titulación académica o título oficial. Además, dado que el artículo no exige que el delito se realice durante la relación de trabajo, sino que se haya tenido acceso a la información con dicho fundamento, bien podría darse más allá de la cesación de la relación laboral o contractual, por lo que el plazo para guardar el sigilo deberá atenerse a la adecuación del tiempo, en aquellos casos de intervalos amplios. Según nos aclara ARROYO ZAPATERO, a diferencia de lo que acaecía en el CPEA de 1973, la revelación de secretos puede proceder

⁴⁷⁵ REQUEJO NAVEROS, Teresa, “El secreto profesional del médico y su protección jurídico penal: una perspectiva histórica”, en Foro – Revista de Ciencias Jurídicas y Sociales Nueva Época, Facultad de Derecho, Universidad Complutense de Madrid, Edit. Marcial Pons, Número 6, año 2007, p.192

tanto del empleador como del empleado, y realizarse tanto en un plano vertical (empleado – empleado), como horizontal (empleado – empleado) o afectar a clientes⁴⁷⁶.

En cambio, el artículo 199. 2 del Código Penal español dice, “el profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años” (la cursiva es nuestra). Se trata de un delito especial propio, con el elemento especial de autoría derivado de la exigencia de que el autor sea profesional esto es que realice una actividad con carácter público y jurídicamente reglamentada⁴⁷⁷, para la cual deberá cumplir requisitos previos, como son estar en posesión de un título académico que lo sustente y, además, poseer el reconocimiento del Estado y el sector propio de la profesión. Siendo así, no sería exigible a una persona que, como apoyo en una urgencia, mantenga el sigilo o reserva de lo que haya visto u oído, pues de no poseer una titulación que lo habilite formalmente para tal acto, no está dentro de los criterios que establece la norma. Tampoco podría exigirse a los estudiantes de medicina que dentro de su práctica conocen de las patologías del paciente y mucho menos al intruso que ejerza ilegalmente una profesión. Asimismo, es importante señalar que el legislador no hace diferencias en el tipo de profesión, pudiendo ser desde abogados, arquitectos, y por supuesto, médicos. En el tema de la medicina moderna, queda claro que esta obligación al secreto no está condicionada a la relación directa o coadyuvante que exista con el paciente, sobre todo por la nueva atención sanitaria “en equipo”, en los que el médico no es el único participante; el resto de profesionales, desde enfermeras o personal de auxilio o el farmacéuta que recibe la receta médica, están compelidos a guardar el secreto de la información que les sea confiada.

⁴⁷⁶ ARROYO ZAPATERO, Luis (Et al), Comentarios al Código Penal, Op. Cit., p. 476 y 477

⁴⁷⁷ STS, 417-2002, de 18 de febrero de 2002, FJ: 2 (RJ 2002\4530)

Nos encontramos ante delitos que protegen el bien jurídico de la intimidad personal⁴⁷⁸, siendo del tipo especiales, puesto que sólo pueden cometerse por un núcleo determinado de personas, siendo necesario que el secreto se conozca como consecuencia de una determinada relación entre la persona que revela el secreto y el titular del mismo⁴⁷⁹, pues para poder realizarse el sujeto activo debe poseer una condición específica, que es tener un oficio o relación laboral; o ser un profesional de una especialidad determinada. A diferencia del art. 197.1 del Código Penal español, que incluye a cualquier persona sin distinción. Según JORGE BARREIRO “el deber de sigilo o reserva profesional ha de estar refrendado por una reglamentación jurídica del ejercicio de la correspondiente actividad profesional (por la ley o por normas estatutarias de la profesión), siendo insuficiente un deber simple ético o moral. Por lo tanto, ha de tratarse de un deber jurídico de sigilo o reserva propio de cada profesión”⁴⁸⁰. Por otro lado, también hay que destacar que el precepto no señala una forma determinada para conocer el secreto, vía documento escrito, oral, o hasta virtual (caso de correo electrónico), etc.; basta que sea conocido por una revelación previa y generalmente voluntaria del sujeto pasivo, quien confía en la reserva de dicha información. Asimismo, otro elemento común entre ambas modalidades delictivas es que sólo cabe su incriminación dolosa, pero no así la culposa⁴⁸¹, tal cual se verá al comentar el elemento subjetivo del delito.

Como elemento diferenciador, en el caso del art. 199 del Código Penal español, el sujeto activo ya conoce el secreto, por lo que la conducta consiste exclusivamente en su divulgación, en hacerlo extensivo a terceras personas⁴⁸². Siendo entonces merecedor de

⁴⁷⁸ JORGE BARREIRO, Agustín, Op. Cit., p. 579

⁴⁷⁹ ALONSO DE ESCAMILLA, Avelina, Op. Cit., p. 188

⁴⁸⁰ JORGE BARREIRO, Agustín, Op. Cit., p. 584

⁴⁸¹ JUANES PECES, Ángel, “Comentarios a los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en CONDE – PUMPIDO TOURÓN (Dir), Op. Cit., p. 1579

⁴⁸² CARBONELL MATEU, Juan y GONZÁLEZ CUSSAC, José, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, Op. Cit., p. 264

especial atención para el legislador, por existir una voluntad de hacer extensiva a terceros no autorizados la información que se entiende protegida. Ahora bien, nuevamente SERRANO GÓMEZ y SERRANO MAÍLLO critican que en estos artículos el tipo es muy abierto y, una vez más, supone inseguridad jurídica. Por la gravedad de las penas se puede llegar en algún caso a violar el principio de culpabilidad.⁴⁸³

Este elemento volitivo no puede dejar de comentarse, pues demuestra la incongruencia con el interés adicional que protege la norma penal. Nos referimos a la confianza que, además, de la intimidad, es requisito indispensable para el ejercicio de la medicina, tal cual lo hemos comentado en los fundamentos históricos. Del mismo modo, está la voluntad del paciente para revelar su intimidad, la cual es inducida y a veces exigida por el propio médico, pues sin dicha información le resultaría más difícil llegar a un diagnóstico efectivo. Siendo así, compartimos lo señalado por GÓMEZ RIVERO cuando señala que es indiferente el dato de la continuidad o no de la prestación desde la óptica del concreto paciente que resulte atendido. Dentro de la actividad profesional habrían de incluirse tanto los casos en que se entabla una relación continuada entre el médico y su paciente como en aquellos otros en que la asistencia es puntual, ya sea porque aquél sólo necesite una primera prestación sanitaria o porque, aun necesitando otras posteriores, rompa expresa o tácitamente la relación con su médico⁴⁸⁴. Y es que en este tema se incluyen también los profesionales de las salas de urgencia, quienes atienden en primer momento al paciente, independientemente que su intervención sólo subsista durante la emergencia del enfermo.

Como quiera que el criterio “profesional”, alcanza a ciertas personas y libera a otras, también hay que señalar que en ciertos casos existe una especial relación de “necesidad” con algunas especialidades, lo que se refuerza con el criterio de protección de la

⁴⁸³ SERRANO GÓMEZ, Alfonso y SERRANO MAÍLLO, Alfonso, Op. Cit., p 287

⁴⁸⁴ GÓMEZ RIVERO, M^a del Carmen, La protección penal de los datos sanitarios, especial referencia al secreto profesional médico, Edit. Comares, año 2007, p. 85

norma penal hacia los ciudadanos. Sobre la propia debilidad del cuerpo humano, se hace inminente la asistencia ante un profesional de la medicina alguna vez en nuestra vida, por lo que es inaplazable que se proteja al enfermo en sus momentos más necesitados.

De igual forma, este artículo 199 del Código Penal español comparte con el tipo general la exigencia de la denuncia previa, al no ser perseguible de oficio, tal como se establece en el artículo 201 del Código Penal español, cuando dice que será necesaria la denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal. En este aspecto podría decirse que pudo darse poca voluntad del legislador en facultar a la autoridad para proteger de manera efectiva el derecho a la intimidad, pues parece dar la espalda a una situación ilegal, amparado en la falta de la presentación de una denuncia. Por otro lado, también podría pensarse en el buen juicio del legislador y cuestionar si realmente tramitar de oficio este tipo de quejas, no pone en mayor riesgo la intimidad del paciente, pues dada la notoriedad del proceso, podría hacerse mayor publicidad y mayor daño al ofendido, con el solo trámite de la investigación.

Sin embargo, si apelamos al tema de marras, tendríamos que destacar que este tipo de delito en su apartado dos, también excluye a los sujetos que no cumplan el perfil de “profesional”, obligando a conocer cuál es la acepción correcta de este término. Es también un delito propio, pues aunque la conducta típica igualmente puede ser realizada por particulares, difícilmente podría sancionarse mediante el art. 199.1 y 2 del Código Penal español.

Sobre el particular, la Real Academia Española de la Lengua define “profesional” como “aquel que ejerce una profesión”. Esta definición es muy escueta, sobre todo por la trascendencia que tiene en la tipicidad y en las exigencias para que se constituya el tipo penal. En ese mismo sentido, MUÑOZ CONDE, señala que cuando el Código Penal se refiere

a un profesional, está aludiendo a un trabajo para cuyo ejercicio se exige un título académico y que conlleva, normalmente, una colegiación, lo que implica el sometimiento a unas normas deontológicas, incluso de carácter profesional disciplinario.⁴⁸⁵ De igual forma, en palabras de SEGRELLES DE ARENAZA, al quedar establecido que el sujeto activo es el profesional, lo que convierte al delito en especial impropio, con las consecuencias que son conocidas, resulta obvio que quien lo contrata no podrá cometer este delito, a diferencia de lo que ocurre en el art. 199.1 Código Penal español, en el que cualquiera de las dos partes integrantes de la relación de trabajo pueden ser sujetos activos. En la práctica, es poco probable que el profesional cuente sus secretos a quien le contrata, pero en caso de hacerlo, la conducta será atípica, salvo que se pueda subsumir precisamente en el art. 199.1 del CPE, lo que exige, a su vez dicho profesional mantenga una relación de trabajo no profesional con el contratante y realice su confidencia en el seno de la misma⁴⁸⁶.

En cuanto a las conductas delictivas, corresponde a revelar en el primer supuesto y divulgar en el segundo, la información que poseen en razón de su especial relación con el paciente. Aquí también se pueden marcar diferencias, aunque en el Código Penal pareciera pretender lo contrario, por ser ambos conceptos idóneos para transmitir información. A nuestro criterio, revelar y divulgar son términos disímiles. Así, revelar es poner en evidencia lo que está oculto, hacer visible lo que no lo estaba. Muy distinto a divulgar, que implica el hacer llegar a uno o más destinatarios una determinada información. Por tal motivo, nos apoyamos nuevamente en la Real Académica de la Lengua, que en estos casos define “revelar” “como el acto de descubrir o manifestar lo ignorado o secreto”, y “divulgar”, “como el acto de publicar, extender, poner al alcance del público algo”.

⁴⁸⁵ MUÑOZ CONDE, Francisco, “Falsedad documental y secreto profesional en el ámbito sanitario”, Revista Derecho y Salud, Volumen 4, número 2, 1996, p. 150

⁴⁸⁶ SEGRELLES ARENAZA, Íñigo, Op. Cit. p. 303

Ahora bien, nos queda identificar cuál es el alcance del verbo divulgar, si basta con la mera actividad para que se consuma el delito, o si requiere que se logre el resultado, para poder hacer típica la conducta. Siendo así, podríamos pensar en el médico que, con intención, dejase a la vista la historia clínica de un paciente, en un sitio de acceso público, con la casi certeza de que al ser un espacio abierto podrá ser vista por terceras personas. Sobre el particular, pensamos que de no consumarse el resultado no cabría señalar la comisión del delito de revelación de secretos. Asimismo, no cabe duda que en este supuesto el médico realiza actividades mediante las cuales libera la información, más no queda a su control quién o quiénes tengan acceso a ella, pues bien podrían verla o no. En este sentido, compartimos criterio con la sentencia del Tribunal Superior de Justicia de La Rioja, cuando dice que el incumplimiento del deber de sigilo, que tanto es como de silencio, secreto o discreción, respecto de asuntos de los que se tiene conocimiento y no deben ser divulgados o revelados, supone que el sujeto a quien se imputa tal incumplimiento conozca la materia secreta o reservada y que, además, la divulgue o revele, siendo esta actuación traslativa a terceros de lo conocido condición “sine qua non”, para que se produzca la conducta infractora, es decir, para que la conducta pueda incardinarse en el tipo sancionador descrito. No siendo bastante el que el secreto o materia reservada se documente, sea por escrito, sea por fijación en otro soporte, siempre que no se haga llegar su contenido a terceras personas, ni quede al alcance de éstas; de donde, el tal deber de sigilo entrañaría el de la debida guarda del soporte documental⁴⁸⁷.

De igual forma, el Tribunal Supremo, mediante Sentencia 574/2001, señala que la acción típica consiste en divulgar los secretos de una persona entendida como la acción de comunicar por cualquier medio, sin que se requiera que se realice a una pluralidad de personas toda vez que la lesión al bien jurídico intimidad se produce con independencia del número de personas que tenga el conocimiento..... Para diferenciar la conducta típica de la mera indiscreción es necesario que lo comunicado afecte a la esfera de la intimidad que el

⁴⁸⁷ STSJ de La Rioja, de 11 de marzo de 1996, FJ: 4 (RJCA 1996\264)

titular quiere defender. Por ello se ha tratado de reducir el contenido del secreto a aquellos extremos afectantes a la intimidad que tengan cierta relevancia jurídica, relevancia que, sin duda, alcanza el hecho comunicado pues lesiona 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 vida humana.⁴⁸⁸

El objeto sobre el que recae la acción es el secreto o información resguardada. Por lo que respecta al tipo subjetivo, es necesario el dolo, que requiere la conciencia y voluntad de la revelar o divulgar el secreto médico. De ahí, nos llama la atención que en ambos apartados, se exige la intención de revelar o divulgar el secreto, y no se hace mención a la imprudencia o la culpa, por lo que de no existir el animus o dolo específico por parte del actor, podría estar fuera de lo establecido en el tipo penal del 199, 1 y 2 del Código Penal español. La intención no va entonces referida al resultado sino a la conducta, y a aquella se une la aceptación del resultado probable o la indiferencia sobre su producción. Habrá que colegirse necesariamente, que el delito carente de tipificación por imprudencia, únicamente se puede cometer intencionadamente y no por imprudencia. La ausencia en el Código Penal vigente de precepto amplio de la entidad del anterior 565, determina que las conductas imprudentes sólo son sancionadas en los casos en que la ley así específicamente lo establezca (así, arts. 152, 267 del Código Penal Español, etcétera)⁴⁸⁹. Ante esta situación, se podría desvirtuar la intención del legislador en proteger la intimidad, en nuestro caso del paciente, mediante el vacío que existe en la redacción del artículo antes comentado. No llevaremos esto a una mayor crítica, pero si nos parece justo recalcar que en el arduo transitar de la protección de los datos y la intimidad del paciente, elementos como el anterior podrían distorsionar el buen ánimo demostrado por el Código Penal español de 1995.

⁴⁸⁸ STS, 574-2001, de 4 de abril de 2001, FJ: 1 (RJ 2001\2016)

⁴⁸⁹ SAP de Guadalajara, 138-2008, 10 de noviembre de 2008, FJ: 4 (ARP 2009\377)

4. Resumen de ideas.

La LOPD 15/1999 y su reglamento, el Real Decreto 1720/2007, han establecido el derecho que tiene el interesado de acceder a la información, especialmente para conocer qué información se tiene sobre sí, y cuál es la fidelidad que existe en la misma.

Aunque el derecho de corrección y oposición están muy vinculados, su campo de acción es diferente, tal como se ha expuesto, y sólo se reconoce actualmente a las personas vivas. De la investigación surge el interés de conocer si estos derechos no pueden ser utilizados por los herederos en caso de fallecimiento del titular, más si se toma en cuenta el amplio criterio aprobado con la intimidad familiar.

La oposición por el contrario está aprobada como una respuesta a la extracción de evaluaciones producto precisamente de la suma de los datos personales que se tengan de un interesado. En múltiples páginas se ha dejado sentado el peligro que existe por la generación de perfiles, al ordenar datos que por separado, a lo mejor no exponen a su titular.

El deber de secreto es la obligación más antigua que se conoce en atención al respecto a los datos personales, su necesidad no ha perdido vigencia y se mantiene la obligación a los profesionales sanitarios, cuando en el ejercicio de su profesión llegan a conocer datos del paciente incluidos en el historial clínico.

Como parte de la investigación, también analizamos aquellos casos en los que se excepciona el deber de secreto y las características muy especiales que debe reunir cada caso para levantar la prohibición de exponer información privada de otros. La ponderación de derechos fundamentales y la posible suspensión de sus efectos se hacen de forma individual, siendo cada caso diferente al resto, por lo que mal se podría hablar en estos casos de la existencia de una norma generalizada aplicable a todos los casos por igual.

CONCLUSIONES

A continuación se exponen las conclusiones finales del presente trabajo de investigación. A lo largo de su desarrollo se analizó el reconocimiento constitucional y legal del derecho a la protección de los datos personales, la importancia y especial defensa de los datos de salud, su incorporación en la historia clínica, además, su vinculación con el derecho a la intimidad y finalmente los medios que están a disposición de las personas (pacientes y usuarios del servicio de salud) para proteger sus datos personales.

De lo anterior, concluimos lo siguiente:

A. Sobre los datos personales.

1. La tecnología ha revolucionado el Derecho, por ende, ahora existen mayores riesgos para las personas y nuevas formas de invadir la privacidad y la confidencialidad de los registros.
2. Aunque el uso de los nuevos dispositivos no conlleva, per se, un efecto negativo para la sociedad, si hay que reconocer que estos adelantos pueden pasar de ser una buena herramienta a un terrible problema. Asimismo, gracias a la tecnología se han podido solucionar múltiples dificultades, pero a la vez se han generado nuevas conductas que son considerados como delitos.
3. Dentro de los primeros capítulos mencionamos especialmente al internet como una herramienta que ha complicado en gran medida la protección de los datos de carácter personal. En la actualidad, este medio es abundantemente utilizado por el Estado y los particulares para compartir información y diariamente los usuarios

del sector público introducen sus datos en ficheros que requieren medidas esenciales a fin de garantizar la integridad y seguridad de esta información.

4. Precisamente, por la gran facilidad de obtener y utilizar la información de las personas, desde cualquier parte del planeta, se expuso en este trabajo, cómo se intenta, mediante nuevas normas, mantener de forma segura los datos personales de sus ciudadanos.
5. No obstante, tal como se mostró en la investigación, la regulación implica una coordinación entre todos los países de la Unión Europea, debido al posible flujo e intercambio de datos entre los países miembros. El movimiento masivo de personas y la liberación de las fronteras también representa una alerta para la seguridad ciudadana.
6. En consecuencia, la atención brindada por el Derecho a estos temas ha sido oportuna y, tanto en la Unión Europea, como en el ámbito interno, se establecieron normativas, leyes y sentencias tan importantes como el Convenio Nº 108, del Consejo de Europa, la Directiva 95/46/CE, del PE y el CUE, la Directiva 97/66/CE del PE y el CUE, la Directiva 2002/58/CE del PE y el CUE, la Ley Orgánica 5/1992 (LOARTAD), la STC 292/2000, la LOPD 15/1999 y el Real Decreto 1720/2007. Todos estos textos resguardan en gran medida el interés del ciudadano por proteger sus datos.
7. De la investigación también resultó que el actual derecho de protección de datos se mantiene en construcción, y aunque se desarrolló la LOPD 15/1999 a través del Real Decreto 1720/2007, aun persisten dudas sobre su nivel de cumplimiento, razón por la cual la Agencia de Protección de Datos se ve en la necesidad de emitir múltiples informes y resoluciones.

8. Por otro lado, tal como vimos en las páginas anteriores, regular el uso de los datos personales generó un amplio debate y, en España, representó diferentes interpretaciones, unas más cercanas al mero reconocimiento de un derecho accesorio, sucintamente mencionado en la Constitución Española (18.4.CE) y otros autores, entre los que me cuento, que nos posicionamos justo en la acera del frente, aquella en la que se reconoce un derecho puro y autónomo, que si bien posee un nacimiento diferente y complicado, eso no le resta la importancia que tiene, más en estos tiempos donde la reserva de la información personal se hace casi imposible.
9. Sobre este tema, la Agencia de Protección de Datos ha jugado un papel importante, a fin de dilucidar conceptos no tan claros en la interpretación jurisprudencial y legal. ¿Qué se protege? ¿el dato o la persona? La respuesta no fue, es, ni será fácil. Con cada informe y resolución se va cimentando el derecho a la protección de los datos, sin desconocer que esto sólo se hace con el fin último de proteger a la personas.
10. En sí, la Agencia de Protección de Datos va sembrando el camino con principios fundamentales para la protección de la información, como son la lealtad, la exactitud, la proporcionalidad y la finalidad, de los cuales surgen procesos administrativos especiales que dan cumplimiento a este nuevo derecho, pero que a la vez resuelven consultas basadas en interrogantes que surgen del diario choque entre particulares y hasta con el propio Estado.
11. En este aparte debo decir que creo en el dinamismo del Derecho y aunque en todo el trabajo se analizó si el derecho a la protección de los datos era o no un derecho autónomo, al final de estas páginas sólo puedo decir que nada en este

mundo es estático, y el Derecho no es una excepción. A lo mejor la protección a la intimidad fue suficiente amparo hace un siglo atrás, pero hoy no está siquiera cerca de cubrir el amplio abanico de posibilidades que ofrece una tecnología mal utilizada.

12. Sobre la norma más actualizada en esta materia, la LOPD 15/1999, desarrollada por el Real Decreto 1720/2007, es importante destacar que ha sido el instrumento jurídico más relevante en los últimos años, sobre todo por su avance frente a la anterior Ley Orgánica 5/1992 (LOARTAD). Esta LOPD 15/1999 significó la trasposición, casi completa, de una directiva comunitaria (Directiva 95/46/CE, del PE y el CUE), aunque con ello no abordó algunos aspectos que ya destacaban como importantes desde la legislación anterior (los datos de salud).
13. Esta LOPD 15/1999 reafirma con gran nitidez los derechos que le asisten a los titulares de la información y, a su vez, impone obligaciones al responsable del fichero y al encargado del tratamiento, por la posible utilización ilegal de los datos de las personas. En cuanto a este último (responsable del tratamiento) limita su participación a los términos establecidos en el contrato que debe suscribir con el responsable del fichero, y si no cumple, se le imponen las mismas sanciones que al responsable principal por el uso de los datos.
14. De este contrato, lo más importante a destacar es que una vez cumplida la prestación de servicios pactada, y cuando ya no sean necesarios para continuar con el encargo realizado, los datos de carácter personal deben ser destruidos. Asimismo, debe ser destruido cualquier registro, respaldo o documento en que conste algún dato de carácter personal objeto del tratamiento.

15. Quedó claro en esta investigación que no cualquiera puede compilar la información de las personas, pues para hacer esto, primero debe declarar su intención ante la Agencia de Protección de Datos, estatal o comunitaria, el tipo de información que posee, los fines que persigue y hasta la vigencia de los mismos. No basta para la ley con la inscripción del fichero, además, deberá garantizar la información oportuna y el consentimiento adecuado de los interesados, como garantía fundamental para su posterior tratamiento, y mientras mantenga la información en sus ficheros, garantizar su protección y la reserva de la misma.

B. Sobre los datos de salud.

1. Aunque proteger todos los datos personales es importante, la investigación desarrollada destacó que dentro de los mismos también existen clasificaciones “por su importancia”, establecidas por la LOPD 15/1999, que distingue la especial sensibilidad en unos y otros. De ahí, que esta investigación continuó su recorrido analizando a los datos de salud, por tener un alto impacto en el titular de la información.
2. Fue precisamente este concepto de datos de salud, el que motivó un amplio debate sobre qué tipo de información podría incluirse en este apartado. Ahora, gracias al Real Decreto 1720/2007 se cuenta con una definición estatal que incluye la salud pasada, presente y futura, física o mental, de un individuo y, en particular, se consideran datos relacionados con la salud de las personas, los referidos a su porcentaje de discapacidad y a su información genética.
3. Con una nueva visión, se plantea el derecho a la protección del dato de salud, desde la premisa de la autonomía o autodeterminación del paciente, lo que deja de lado el paternalismo médico que durante años imperó en los sistemas de atención de salud.

La superación del paternalismo fue el resultado de un largo proceso histórico que finalmente se incorporó a la medicina, con la aprobación de la LOAP 41/2002, en la cual el paciente es competente para decidir sobre sus datos de salud.

4. Como resultado de esta investigación también debemos señalar que, de ser posible, consideramos positivo incluir definiciones exactas en las normativas que desarrollan los temas de salud, y evitar la incorporación reiterada de conceptos muy abiertos sujetos a múltiples interpretaciones. En el caso del dato de salud es muy importante que la ley defina, con claridad meridiana, cuál es su alcance, ya que por mucho tiempo esta falta de definición pudo facilitar la comisión de actos en contra del derecho de las personas.
5. Como quiera que se ha mantenido el concepto dato de “salud” como eje central de este trabajo, también hay que decir que durante la investigación nos encontramos con otros conceptos “parecidos” o que por lo menos intentaban incorporar esta materia, como son los datos “sanitarios”, “médicos y “hospitalarios”, entre otros. Pero, tal cual lo explicamos en el texto del trabajo, lo más acertado en estos casos será utilizar el dato de “salud”.
6. Como complemento a la normativa de protección de los datos, este trabajo también se apoya en la LOAP 41/2002, norma fundamental de derechos del paciente. Esta normativa también desarrolla, a nivel estatal, criterios esenciales de la historia clínica (siguiente capítulo en análisis), los derechos del paciente y sobre todo, las alternativas que posee el enfermo en cuanto a su tratamiento médico.
7. Esta LOAP 41/2002 aportó soluciones importantes en materia de menores de edad, sobre todo por los derechos que le asisten a este tipo de paciente cuando reciben tratamientos médicos en clínicas, hospitales y otros. Su importancia se destaca por

desarrollar la materia del consentimiento informado y los permisos que se deben obtener, antes de participar a los padres sobre las condiciones de salud de su hijo. Sin embargo, el hecho de establecer periodos y edades para determinar la capacidad plena de este tipo de paciente, aun no deja de generar disquisiciones conceptuales, lo que aun causa algunas incomodidades especialmente en el tema del aborto.

8. Otro aspecto importante dentro del trabajo son los datos de salud genéticos. En este apartado se destaca que este tipo de datos están muy vinculados con el avance tecnológico, y que producto de su uso, no sólo revelan información del paciente, presente y futura, sino que también están en la capacidad de revelar información de los familiares, aun cuando éstos no hayan prestado su consentimiento para ello. En sí, la información sobre el genotipo de una persona descubre su “esencia” más íntima y, por tanto, merece ser protegida con el régimen especial que exige la LOAP 41/2002.
9. En la investigación destacamos la importancia de los datos genéticos para detectar oportunamente la existencia de enfermedades, pero la elaboración de los “bio bancos” y la conservación de las muestras, también merece que se imponga con gran rigurosidad la obtención del consentimiento expreso y específico por escrito para realizar el análisis genético.
10. Un mal uso de la información genética desencadena en escenarios de discriminación, por la predisposición a enfermedades que, a lo mejor, ni siquiera llegue a desarrollar el paciente, pero que existen de forma recesiva en su cuerpo. Estas exclusiones abarcan no solamente el entorno social, sino los beneficios de reclutamiento y conservación del trabajo, la aplicación o beneficios de ciertos seguros, entre otros.

11. En este sentido, el trabajo de investigación resalta lo indispensable que es disociar los datos de salud, previo a su utilización para propósitos distintos a la atención del paciente, salvo que éste último haya consentido el uso íntegro de su información de salud. La propia Agencia de Protección de Datos señaló que no basta con establecer códigos simples para cumplir con esta obligación, sino establecer mecanismos tan complicados, que desanime a cualquier persona, ajena al paciente, a descifrar la información de otros.

12. De no contarse con tal esfuerzo desproporcionado, el fichero queda automáticamente bajo la regulación de la LOPD 15/1999, con las consecuentes obligaciones para el responsable del fichero. En este aspecto lo importante es que toda esta labor sea realizada por personal cualificado en centros acreditados que reúnan los requisitos de calidad y seguridad.

13. Aunque en la investigación hemos mencionado derechos y obligaciones de ambas partes (titulares de la información y responsables del fichero), un derecho es de especial relevancia en nuestra opinión. Se trata del consentimiento informado del paciente. Ha de aclararse que esta investigación sólo analizó el consentimiento informado para el uso de la información de salud más allá de la atención clínica (judicial, docencia, investigación, estadística), no el consentimiento informado regulado en la LOAP 41/2002, que se refiere a los tratamientos médicos, por ser materias totalmente diferentes.

14. Este consentimiento informado para el uso de los datos de salud, no solo es obligatorio en hospitales y centros de atención sanitaria en general, también es exigible en otros sitios, como es el caso de los centros de trabajo, donde la oficina de recursos humanos, por ejemplo, debe contar con el consentimiento de sus

empleados, previo a utilizar su información para otros propósitos, distintos a los fines que justificaron su recolección.

15. En todo caso, aunque la LOPD 15/1999, el Real Decreto 1720/2007 y la LOAP 41/2002, son normas de carácter estatal y de claro cumplimiento en todo el territorio español, esto no fue impedimento para que las Comunidades Autónomas desarrollaran, de manera interna, otros beneficios para sus ciudadanos y proteger así, de manera integral, todos los derechos de las personas a la confidencialidad de sus datos.

C. Sobre la historia clínica.

1. La historia clínica es el compendio de información relativa a la salud del paciente y que resulta fundamental para su adecuada atención terapéutica. En el desarrollo de esta investigación se optó por analizar este documento por considerar que constituye un ejemplo claro de archivo de diversos datos personales, entre ellos los datos de salud, columna vertebral de este trabajo.
2. La historia clínica estuvo regulada inicialmente por la LGS 14/1986 y, posteriormente, por la LOAP 41/2002. En la LOAP 41/2002 se desarrollan elementos fundamentales como son la forma de constituir este dossier, los documentos principales que la componen, los derechos de acceso, los plazos de vigencia o conservación y, sobre todo, aspectos sobre su control o tenencia. Aunque esta LOAP 41/2002 es de gran ayuda para la defensa de los derechos del paciente, aun persiste la crítica de que, en dos artículos (3 y 14.1) desarrolla diferentes conceptos de historia clínica, en el primero más corto que el segundo. Esta doble definición abre nuevamente el debate en cuanto a su alcance.

3. La LOAP 41/2002 señala que es obligación de cada centro sanitario constituir una historia clínica por cada paciente, razón por la cual debe poder identificarse de manera sencilla pero eficiente, mantener criterios de control de acceso a su contenido, estar actualizada con cada tratamiento aplicado al paciente y sobre todo, estar custodiada en sitio seguro sin riesgos de alteración, pérdida o destrucción.
4. Sin embargo, aunque la LOPD 41/2002 resolvió que la historia clínica debe conservarse en los hospitales o centros de atención sanitaria, aun persiste el debate sobre quién ostenta la propiedad del expediente. El paciente insiste en ser el sujeto que le da vida a dicho conjunto de documentos, el médico defiende su “autoría” y el hospital su derecho a resguardar tal documento. Tal como mencionamos en páginas anteriores, somos del criterio de que cada uno es titular de un derecho sobre este documento y no un “propietario”, como si de un bien económico se tratase. En sí, estos derechos son complementarios y coexisten a la vez, por lo que pueden reclamarse paralelamente.
5. La vigencia de este documento ha sido establecida de manera general por la LOAP 41/2002 en cinco años, aunque tal parámetro no impide que las Comunidades Autónomas puedan establecer, de manera independiente, plazos mayores, siempre y cuando, quede asegurada su autenticidad e integridad. El plazo de cinco años nos parece algo corto, debido al lento trámite que a veces se asigna a las reclamaciones por casos de mala praxis médica. En este tema creemos que sería positivo plantear un periodo más amplio, dado que se cuenta con la tecnología que facilita su conservación.
6. Si en el capítulo de los datos de salud el consentimiento informado era tema de especial interés, en el capítulo de la historia clínica este lugar lo ocupa la confidencialidad de la información. Durante toda la investigación desarrollamos la

importancia de mantener en reserva esta información y no permitir que la misma sea de libre distribución entre los particulares. Tal como hemos visto, el secreto no es absoluto y en la práctica médica pueden surgir situaciones de conflicto entre el deber de secreto y el principio de beneficencia del médico, que a la vez es una fuerte protección legal del derecho a la intimidad.

7. Precisamente el tema del acceso a la historia clínica mantiene el debate sobre la entrega total de este compendio al paciente, dado que la LOAP 41/2002 sostiene la obligación de reservar las anotaciones subjetivas de los médicos, razón por la que el paciente aun puede reclamar su derecho a recibir un documento íntegro y no una selección de páginas. Una queja analizada en esta investigación es la limitada capacidad de defensa que tiene el paciente, si no recibe de forma íntegra su historia clínica.
8. La tecnología también se hace notar en la historia clínica y en la actualidad se está abandonando el sistema de compilación de datos, mediante sistema físico, para utilizar los historiales clínicos electrónicos, cuya conservación es más eficiente, por no ocupar tanto espacio y no sufrir el deterioro que sucede con el papel, además que se puede compartir más rápido y de forma paralela entre distintos profesionales de la salud. Ahora bien, la desventaja de una posible pérdida parcial o total siempre estará latente, por eso es importante establecer respaldos adecuados, que se actualicen constantemente con la actividad del paciente.
9. Establecer historiales clínicos de forma electrónica también conlleva otras desventajas, como es elevar los controles de seguridad en cuanto al acceso. Cada usuario de este documento debe contar con una contraseña que permita rastrear quiénes han ingresado a su contenido y, más de allá de saber quién atiende al

paciente, se debe garantizar la trazabilidad de los cambios efectuados, para conocer quién ha realizado modificaciones.

10. En consecuencia, la fidelidad y la confidencialidad de la información son los retos más importantes que deberá afrontar este nuevo sistema de compilación de los datos de salud. De ahí que los hospitales y centros sanitarios que se acojan a este sistema electrónico, deben garantizar ante la Agencia de Protección de Datos los suficientes niveles de seguridad y los controles de acceso que debe tener con cada expediente de sus pacientes, para evitar el acceso de “piratas informáticos”, que posteriormente puedan poner en peligro la seguridad de la información obtenida del paciente.

D. Sobre el derecho a la intimidad

1. El derecho a la intimidad es el más vinculado con el nuevo derecho a la protección de los datos personales, quizás porque ambos fueron considerados por mucho tiempo como un solo derecho fundamental. Sin embargo, dentro de la investigación se pudo comprobar que aunque comparten elementos parecidos y se mantienen muy relacionados, en el fondo son muy diferentes entre sí.
2. El derecho a la protección de los datos y el derecho a la intimidad poseen una característica especial dentro de los derechos fundamentales, y es que ambos son derechos de los que el sujeto se puede despojar voluntariamente. Esta característica supone una gran diferencia con otros bienes jurídicos protegidos, por ejemplo, el derecho a la vida y el derecho a la salud, entre otros, que no cuentan con tal permiso legal.
3. No todos los datos personales son datos íntimos. Este fue uno de los fundamentos esenciales que utilizó la STC 292/2000 para diferenciar la intimidad del derecho

fundamental a la protección de los datos. Esta sentencia señaló que 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 estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, permitiendo también al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

4. Por otro lado, el derecho a la intimidad es también un elemento esencial en la constitución de la historia clínica. Su importancia radica en el tipo de información sensible que corresponde a los pacientes mientras reciben tratamiento en los centros sanitarios. La investigación demostró que este aspecto también es difícil de cumplir, especialmente por la masiva asistencia de los pacientes a los centros hospitalarios, lo cual impide que haya suficiente espacio entre los enfermos hospitalizados, siendo difícil al menos garantizar la intimidad corporal.
5. También es importante señalar que aunque el término “privado”, se utiliza como sinónimo de lo íntimo, dentro de la investigación se pudo comprobar que estos términos tampoco son iguales, debido a que lo privado se ubica en contraposición de lo público, en tanto que lo íntimo hace referencia a lo que simplemente no se comparte, como el pensamiento o las ideas, independientemente si nos rodeamos de otras personas. De ahí que no todo lo privado es íntimo, pero todo lo íntimo sí es privado.
6. Con todo y lo anterior, la intimidad, en todas sus variantes, se encuentra entre los conceptos más difíciles de definir, debido a que responde al criterio de cada persona, siendo mayor o menor su ámbito de cobertura, dependiendo de a quién se consulte. Este derecho está vinculado directamente con la personalidad del sujeto, por ende, se extingue con el fallecimiento de cada sujeto.

7. Sobre el fallecimiento del titular, dentro de la investigación dejamos claro que, aunque respetamos el criterio de la extinción del derecho a la intimidad con la muerte de la persona, creemos adecuado y necesario el amparo que se ha dado a los familiares, con la extensión de este derecho a una “intimidad familiar”, que proteja a los parientes luego de la muerte de su familiar.
8. Aunque el respeto al derecho a la intimidad está debidamente sustentado en las historias clínicas, debe señalarse que también tiene sus límites. Por tanto, no es un derecho absoluto y puede ser suspendido, mediante ley, por causas de interés general. Por ejemplo, cuando se trate de enfermedades infecto contagiosas (como el caso del SIDA, en el que el informe de la misma es obligatorio) y los casos de epidemias, en los que el interés de preservar la salud de la población en general prevalece ante todo.
9. En este trabajo también señalamos cómo el derecho a la intimidad colisiona constantemente con otros derechos como son, el derecho a la información o inclusive la libertad de expresión. Sobre esto, en el trabajo se plantearon las condiciones mínimas que deben existir para que la información de salud de un particular pueda publicarse en los medios, bajo el amparo del derecho a la información. Tales requisitos esenciales son: el consentimiento previo, y, de no ser posible, la disociación de los datos.
10. De igual forma, los derechos a la intimidad y la libertad se ven constantemente amenazados por los intensos controles de seguridad que se aplican por parte de las autoridades. Para evitar posibles riesgos a la sociedad, se ha hecho común generar ficheros con diversos tipos de datos, creando perfiles que los ciudadanos desconocen

y que posteriormente podrían determinar si les limitan otros derechos constitucionales.

11. En este trabajo se analizaron diferentes tipos de intimidad como son, la intimidad corporal y la intimidad económica. La intimidad corporal es aquella que usualmente se pierde con el tratamiento médico y en ocasiones hasta corre peligro con las revisiones que ejecuta la policía al realizar los arrestos (por ejemplo, casos de ingesta de drogas). En este trabajo dejamos claro que la intimidad corporal no es un blindaje que proteja al sujeto por la comisión de delitos, pero para realizar alguna revisión al cuerpo, primero debe ser ordenado por autoridad competente y darse conforme a los criterios de confidencialidad que exige la ley.

Asimismo, la intimidad económica se pierde en aquellos casos donde el Estado ingresa a las cuentas bancarias de los ciudadanos para tener el control sobre el movimiento de los fondos de dinero. Este dominio de la libertad económica se da cuanto existe riesgo de terrorismo o lavados de dinero, ambos delitos plenamente tipificados en las normas penales.

12. La confidencialidad de la información, se transforma en una obligación de secreto sobre lo conocido, en razón del ejercicio de la profesión. Esta obligación corresponde al responsable del fichero por los datos que posee de los particulares. De igual forma, el médico, por la confección de la historia clínica. Y cualquier individuo, profesional o no, que, por razones de las tareas que realiza, tenga conocimiento de datos íntimos de una persona. En este sentido, el Código Penal español incorpora dentro del tipo penal aquellos casos en los que responsable de guardar el secreto sea un profesional y aquellos en los que es un particular. En ambos casos, tal como se expuso en el trabajo, establece penas acorde con las conductas realizadas por las personas.

E. Sobre los medios para proteger los datos de salud del paciente

1. La LOPD 15/1999 y el Real Decreto 1720/2007 también establecen medios de control, ante la afectación de los ciudadanos en el uso de sus datos personales. Un aspecto importante que analizó este trabajo es la obligación del responsable del fichero de informar al interesado sobre la existencia del fichero y ante quién presentar sus quejas o consultas. Conforme a esta obligación, se puede entablar, de forma adecuada, los medios de defensa del titular de los datos.
2. La información y el consentimiento son métodos previos de protección, dado que ambos impiden que se obtengan datos sin el conocimiento de su titular. En ambos casos, atañe al responsable del fichero demostrar que informó adecuada y suficientemente al titular de los datos (paciente) sobre los fines o propósitos para recolectar los datos. Asimismo, que se concede el consentimiento, en consecuencia, de manera libre y sin ningún tipo de presión.
3. Con posterioridad a la recolección de los datos, existen otros medios que garantizan a las personas el poder de control sobre sus datos, estos son: los derechos de acceso, rectificación, cancelación y oposición. Mediante estos derechos se impone a al responsable del fichero un deber de hacer, según la propia necesidad del titular de los datos.
4. Dentro de la investigación se abordó la importancia de ejercer estos derechos personalmente, salvo que se cuente con representación legal debidamente constituida o por un representante acreditado (casos de personas con discapacidad y/o menores de edad). Sobre lo anterior, la propia Agencia de Protección de Datos ha dejado claro que no son válidos los apoderamientos generales, por lo que debe facultarse expresamente al representante, si se desea hacer uso de estos derechos.

De no cumplir con este aspecto, estará el responsable del fichero facultado para denegar estos derechos cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que actúa en su representación.

5. Tal como hemos mencionado en todo este trabajo, todos estos derechos cuentan con plazos establecidos por el Real Decreto 1720/2007. Por ejemplo, 12 meses en el caso del derecho de acceso. Y para ser presentados deben utilizarse procedimientos sencillos, que faciliten al titular de los derechos la presentación de sus quejas o consultas.
6. Cabe señalar que dentro de la lectura de trabajos doctrinales se detectaron algunas críticas a la LOPD 15/1999 por utilizar el concepto “interesado”, dado que no es lo mismo que “titular” de los derechos. Sobre lo anterior la queja principal radica en que ser interesado implica a muchas personas independientemente de su vinculación a la información, además, que riñe con la obligación de ejercitar los medios de manera personalísima.
7. En cuanto al derecho de acceso, la LOAP 15/1999 y el Real Decreto 1720/2007 facultan al afectado a obtener información sobre sus propios datos, y, especialmente, a conocer si los mismos son objeto de tratamiento, la finalidad del mismo, así como la información de cómo se obtuvieron. Dentro de los informes de la Agencia de Protección de Datos se encuentra la obligación del responsable del fichero de asegurarse sobre quién solicita la información, antes de revelarla.
8. En igual sentido, se concluye que el derecho de acceso también puede ser restringido, como en los casos de estado de necesidad terapéutica. En estos casos, el médico vuelve a su rol paternalista y, si considera que entregar la información completa del estado de salud del paciente le traerá negativas consecuencias, podría reservar parte

de la información en beneficio del propio enfermo. Esta opción, legalmente constituida en la LOAP 41/2002, también recibe críticas, ya que el paciente tiene derecho a conocer toda su información, independientemente de lo grave que sea.

9. Los derechos de rectificación y cancelación buscan, en el primer caso, modificar los datos que resulten ser inexactos o incompletos y, en el segundo caso, suprimir los datos que resulten ser inadecuados o excesivos. Según la normativa vigente, ya mencionada en apartados anteriores, ambos procesos deben resolverse en el término de diez días y deben señalarse con exactitud a qué información “errónea” se refiere, a fin de que el responsable del fichero pueda cumplir adecuadamente con sus obligaciones. De igual forma, toda solicitud se basará sólo en la información que se refiere a la persona solicitante, siendo ilegal hacer cambios en datos ajenos.
10. El derecho de cancelación estará sujeto a los términos que establecen las leyes respectivas para cada caso. Por ejemplo, en lo relativo a los datos de salud, incluidos en el historial clínico, debe cumplirse el mínimo de 5 años impuestos por la LOAP 41/2002. Asimismo, el propio responsable del fichero puede cancelar de oficio la información que posee; si comprueba que la misma no está actualizada y podría causar algún inconveniente al titular de los datos. Ahora bien, este cambio o ajuste no necesariamente implica reemplazar un dato nuevo por uno viejo y borrar todos los antecedentes. Por el contrario, bastaría con enviar el dato reemplazado a un registro histórico, hacer constar desde cuándo se hicieron los cambios y cómo se obtuvo la información actualizada y así conservar toda la información que se tiene de la persona, como una secuencia ordenada de datos personales.
11. Tal como se mencionó en el desarrollo de la investigación, con en el derecho de oposición se prohíbe al responsable del fichero llevar a cabo el tratamiento de los datos o se pide suspender el mismo, en aquellos supuestos en los que no sea

necesario su consentimiento para el tratamiento. Por ejemplo, los ficheros de intereses bancarios o financieros, basados en el perfil que arroje el manejo de los datos del titular de la información.

12. Así como en el caso de la intimidad de las personas, se amplió el amparo a los familiares mediante la idea de una “intimidad familiar”, somos del criterio que esto también podría aplicarse para el derecho de acceso y rectificación que podrían tener los familiares de una persona fallecida. La LOPD 15/1999 y el Real Decreto 1720/2007 reconocen el derecho de cancelación de los herederos, pero dejan de lado, a nuestro criterio, otros derechos tan importantes como el acceso y la rectificación.
13. De igual forma, la investigación también contempló la obligación del secreto profesional, como primera alternativa que tiene el paciente para conservar de forma reservada su información. Como quiera que callar y no hablar serían consecuencias dimanantes del secreto médico, está claro que acogerse a un derecho de no hablar ha sido uno de los aspectos más controvertidos de esta investigación, pues a diferencia de la profesión del abogado, por ejemplo, el médico si tendría que develar la información que conoce, si es requerido por autoridad judicial.
14. Esta obligación de callar se traslada con cada profesional de la medicina que conozca del historial clínico del paciente, sobre todo en los casos de medicina en equipo. En estos supuestos, todos los médicos estarán obligados a reservar la información de su paciente y evitar su divulgación o conocimiento, por parte de terceros, de los hechos, situaciones, comportamientos e informaciones que la persona desea mantener reservada para sí o para el núcleo familiar.
15. De todo lo anterior, también existirán condiciones que liberan al médico de su gran carga, la confidencialidad. Por ejemplo, la autorización del paciente, la declaración

obligatoria de enfermedades y la revelación del secreto a favor del propio médico, entre otras. En cada caso, el derecho administrativo sancionador y el derecho penal pueden intervenir, a fin de determinar si se ha cumplido con las excepciones de rigor o si, por el contrario, se está ante una clara violación de los derechos que asisten al sujeto, ante el resguardo de sus datos personales.

En conclusión, en los últimos años la protección de los datos ha revolucionado diferentes áreas del Derecho, lo que ha fomentado a la vez el surgimiento de nuevas formas o estrategias legales para salvaguardar la libertad, la privacidad y la dignidad de las personas.

Esta urgencia por regular la protección de los datos personales, tiene su base en la materialización de una preocupación actual y concreta que, desde un punto de vista meramente jurídico, llega a abarcar una amplia gama de derechos de las personas. La tecnología ha desbordado los márgenes de afectación a las personas, por lo que una protección adecuada y efectiva se requiere con prontitud.

La sociedad contemporánea en la que vivimos, ampliamente bombardeada con el cruce libre de información, exige la reivindicación de la esfera íntima de los particulares, sus datos personales, especialmente en aquellas áreas consideradas sensibles, como son los datos de salud. La información de salud, a diferencia de otros tipos de datos, puede compartirse repetidas veces sin que se desgaste ni se pierda y allí radica el peligro para las personas. Estas características causan un serio conflicto con la confidencialidad que se exige en este tipo de datos, debido a la propia naturaleza y características de la información y de los diferentes ámbitos de su utilización, tal como hemos visto durante toda la investigación.

Solo podemos recalcar que es importante que los ciudadanos tomen conciencia del grave peligro que asumen al compartir libremente y sin protección, sus datos personales,

principalmente porque pueden verse sometidos a decisiones que escapan a su control y decisión.

BIBLIOGRAFÍA CITADA

ABERASTURI GORRIÑO, Unai y LASAGABASTER HERRARTE, Iñaki, “La cesión de datos de salud fuera del ámbito sanitario. Análisis de supuestos concretos en que la información sanitaria se transmite para el cumplimiento de fines distintos al de la protección de la salud de las personas”, en Revista Vasca de Administración Pública, Núm. 91, Septiembre Diciembre, 2011, pp. 17 – 102

ABERASTURI GORRIÑO, Unai, “Movimiento internacional de datos. especial referencia a la transferencia internacional de datos sanitarios”, en Revista de Administración Pública, Núm. 186, Septiembre – Diciembre, 2011, pp.329 – 369

AGUSTINA SANLEHI, José R., El delito de descubrimiento y revelación de secretos en su aplicación al control del correo electrónico del trabajador, Edit. La Ley, 2009, P 96 – 97.

ALMUZARA ALMAIDA, Cristina, “Relaciones pre contractuales y contractuales”, en ALMUZARA ALMAIDA, Cristina, Estudio práctico sobre la protección de datos de carácter personal, Lex Nova, pp. 88 – 224

ALONSO ÁLAMO, Mercedes, “El consentimiento informado del paciente en el tratamiento médico. Bases jurídicas e implicaciones penales”, en MENDOZA BUERGO, Blanca (Editora), Autonomía personal y decisiones médicas, Thomson Civitas, 2010, pp. 97- 141

ALONSO DE ESCAMILLA, Avelina, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en LAMARCA PÉREZ, Carmen (Coord.), Derecho penal parte especial, Edit. Colex, Madrid, 2008, pp.181 - 194

ALONSO OLEA, Manuel y FANEGO CASTILLO, Fernando, Comentario a la ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, Edit. Thomson, 2003, p. 63

ÁLVAREZ – CIENFUEGOS SUÁREZ, José María, Aspectos jurídicos y protección de datos sanitarios, resumen de la II jornada madrileña de admisión y documentación médica. Madrid, Fundación Hospital de Alcorcón, 20 de mayo de 1999; p.59.

ÁLVAREZ De NEYRA KAPPLER, Susana, “El consentimiento en la toma de muestras de ADN. Especial referencia a los procesos de menores (parte II), en Revista de Derecho y Genoma Humano, Universidad de Deusto, Núm 35, Julio – Diciembre, 2011, pp. 41 – 65

ALVAREZ GONZÁLEZ, Susana, “El habeas data biosanitarios: especiales situaciones de conflicto en relación con los datos genéticos, en GARRIGA DOMINGUEZ, Ana y ÁLVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos personales, especial referencia al registro obligatorio de los portadores del VIH, Dykinson s.l. 2011, pp.51 – 70

ALVARÉZ GONZÁLEZ, Susana, Aspectos éticos y jurídicos de la comunicación de datos del paciente con VIH/sida a terceros interesados en la información, en GARRIGA DOMINGUEZ, Ana y ÁLVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos personales, especial referencia al registro obligatorio de los portadores del VIH, Dykinson S.L. 2011, pp.155 - 179

ÁLVAREZ HERNANDO, Javier, Guía práctica sobre protección de datos, cuestiones y formularios, Lex Nova, 2011, p. 54

APARICIO SALOM, Javier, Estudio sobre la ley orgánica de protección de datos de carácter personal, Edit. Aranzadi, 2000, pp. 48 y 49.

APARICIO SALOM, Javier, Estudio sobre la ley orgánica de protección de datos de carácter personal, Aranzadi, 2002, p.153. Ídem, VÍZCAINO CALDERÓN, Miguel, Comentarios a la ley orgánica de protección de datos de carácter personal, Civitas, 2001, p.195

ARENAS RAMIRO, Mónica, El derecho fundamental a la protección de datos personales en Europa, Tirant Lo Blanch, 2006, p. 55

ARROYO ZAPATERO, Luis (Et Al), Comentarios al código penal, Edit. Iustel, Madrid, p. 472

ARTAL, Roser, “La informatización de los datos de salud”, en RIPOL CARULLA, Santiago (Ed.), estudios de protección de datos de carácter personal en el ámbito de la salud, Marcial Pons, 2006, pp. 105 – 119.

AYERRA LASCANO, José M., “Regulación general de la historia clínica”, en Revista Derecho

y Salud, volumen 11, Número 1, Enero – Junio 2003, pp. 23 - 38

AYERRA LAZCANO, José M., “Regulación general de la historia clínica”, en Revista Derecho y Salud, volumen 11, número 1, enero junio 2003, p.28

BALLESTEROS MOFFA, Luis Ángel, La privacidad electrónica Internet en el centro de protección, Tirant Lo Blanch, 2005, p.142

BEJAR, Helena, El ámbito íntimo. privacidad, individualismo y modernidad, Edit. Alianza, Madrid, 1995, p. 44

BELTRAN AGUIRRE, Juan L., “Tratamientos de datos de salud en la prestación de servicios sociales”, en Revista Derecho y Salud, volumen 18, número 1, enero – junio, 2009, pp. 1-20

BENTHAM, Jeremy. “Deontology together with a table of springs of action and article on utilitarianism, Edit. Amnon Goldworth, 1983, p. 119

BERTOLINO, Rinaldo, “La cultura moderna de los derechos y la dignidad del hombre”, en Revista de Derechos y Libertades – Revista del Instituto Bartolomé de las Casas, año IV, enero 1999, número 7, pp. 131 - 139

BUSTOS PUECHE, José Enrique, En su obra manual sobre bienes y derechos de la personalidad, Año 1997, Edit. Dykinson.

ČAS, Johann, “Computación ubicua, privacidad y protección de datos: opciones y limitaciones para reconciliar contradicciones sin precedentes”, en Revista Española de Protección de Datos, núm. 6, Enero – Junio, 2009, pp. 69 – 104

CASTELLANO ARROYO, María, “Problemática de la historia clínica”, en información y documentación clínica, Madrid, Consejo General del Poder Judicial y Ministerio de Sanidad y Consumo, 1997, Vol. I, pp. 45 – 90

CATILLO JIMÉNEZ, Cinta, “Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información”, en Derecho y conocimiento, Anuario Jurídico sobre la Sociedad de la Información, Volumen 1, Universidad de Huelva, 2001, pp. 35 - 48

CERRILLO I MARTÍNEZ, Agustí, “La difusión de información pública en internet”, en CERRILLO I MARTÍNEZ, Agustí, Et Al, La administración y la información, Marcial Pons, 2007, pp. 11-39

CONCEPCIÓN HERNANDEZ, José Luis, Honor, intimidad e imagen, un análisis jurisprudencial de la LO. 1/1982, Bosh, 1996, p. 43

CONDE ORTIZ, Concepción, la protección de datos personales, un derecho autónomo con base en los conceptos de intimidad y privacidad, Dykinson, 2005, p. 29

CONTRERAS MAZARÍO, José M., “Derecho a la intimidad, pruebas biomédicas y relaciones laborales. Especial referencia a la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas”, en Derechos y Libertades, Revista del Instituto Bartolomé de las Casas, Universidad Carlos III, Año V, Julio/Diciembre, 2000, Número 9, pp. 189 - 223

CÓRDOBA RODA, Juan, Abogacía, secreto profesional y blanqueo de capitales, Edit. Marcial Pons, Madrid/Barcelona, 2006, p. 32

CORRIPIO GIL-DELGADO, María De Los Reyes, Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet, Agencia de Protección de Datos, 2000, p.134

CREVILLÉN SÁNCHEZ, Clemente, Derechos de la personalidad. honor, intimidad personal y familiar y propia imagen en la jurisprudencia, Doctrina y Jurisprudencia, 1996, p. 75

CRUZ, Juan, El éxtasis de la intimidad. Ontología del amor humano en Tomas de Aquino, Madrid, Edit. Rialp, 1999; p. 16

CUESTA PASTOR, Pablo, “Los mecanismos de identificación y su uso en el proceso penal: interrogantes a propósito de la huella de ADN”, en ROMEO CASABONA, Carlos (Editor), Bases de datos de perfiles de ADN y criminalidad, Edit. Comares S.L., Granada, 2002, pp.75 - 124

CURIL HERRERO, Jesús y ESTÉVEZ LUCAS, Joaquín., Manual para la gestión sanitaria y de historia clínica hospitalaria, Editores Médico S.A., 2000, p. 27.

DAVARA FERNÁNDEZ DE MARCOS, Isabel, Hacia la estandarización de la protección de datos personales, La Ley, 2011, p. 360

DAVARA RODRÍGUEZ, Miguel A., Guía práctica de protección de datos, desde la óptica del titular del fichero, Universidad Pontificia de Comillas, 1999, p. 66

DAVARA RODRÍGUEZ, Miguel A., La protección de datos personales en el sector de las telecomunicaciones, Universidad Pontificia de Comillas, 2000, pp. 13 y 14

DE LORENZO Y MONTERO, Ricardo, “Propiedad y destino de los resultados de las investigaciones médicas, cuestiones referentes a la historia clínica”, en MARTÍNEZ MORÁN, Narciso (Coord.), Biotecnología, derecho y dignidad humana, Edit. Comares, Granada, 2003, pp.289 - 308

DE MIGUEL SÁNCHEZ, Noelia, “Intimidad e historia clínica en la nueva ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica”, en Civitas, Revista Española de Derecho Administrativo, Número 117, Año 2003, pp. 9 - 31

DE MIGUEL SÁNCHEZ, Noelia, Secreto médico, confidencialidad e información sanitaria, Edit. Marcial Pons, 2002, pp. 89 y 90

DE TOLEDO Y UBIETO, Emilio, Algunas reflexiones sobre el tratamiento jurídico del secreto profesional, en Revista La Ley, Volumen 1, 1983, pp. 1137 – 1139

DEL CASTILLO VÁZQUEZ, Isabel-Cecilia, Protección de datos: cuestiones constitucionales y administrativas – el derecho a saber y la obligación de callar, Thomson Civitas, 2007, pp.143 Y 144

DÍAZ –PICAZO, Luis María, Sobre secretos oficiales, Civitas, 1998, p. 37

DIAZ REVORIO, Javier, “El derecho fundamental al secreto de las comunicaciones”, en revista de derecho PUC, Edit. Fondo, Nº 59, 2007, p. 162

DOMÍNGUEZ LUELMO, Andrés, Derecho sanitario y responsabilidad médica, Edit. Lex

Nova, 2003, p .401

DOMÍNGUEZ MARTÍN, Mónica, Formas de gestión de la sanidad pública en España, La Ley, 2006.

EGUSQUIZA BALMASEDA, Ma. Ángeles, Protección de datos: intimidad y salud, Aranzadi, 2009.

FARIÑAS M., Luis, El derecho a la intimidad, Madrid, Edit. Trivium, 1983, p.327

FERNÁNDEZ COSTALES, Javier, “Intimidad de la persona y confidencialidad de datos en el marco de la vigilancia de la salud. El respeto a los derechos del trabajador en los reconocimientos médicos”, en Revista Derecho y Salud, Volumen 16, Número 1, Enero – Junio 2008, pp. 81 - 108

FERNÁNDEZ LÓPEZ, Juan M., “El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario”, en Revista Derecho y Salud, Extraordinario XI Congreso Derecho y Salud, Volumen 11, Mayo 2003, pp. 37 – 46

FERNÁNDEZ PROL, Francisca, “análisis de la discriminación por enfermedad en el ámbito laboral. especial referencia al caso del SIDA”, En GARRIGA DOMINGUEZ, Ana y ÁLVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos personales, especial referencia al registro obligatorio de los portadores del VIH, Dykinson S.L. 2011, pp.135 – 153

FRIGOLA VALLINA, Joaquín y ESCUDERO MORATALLA, José, Honor, secreto profesional y cláusulas de conciencia en los medios de comunicación. Límites y aspectos jurídicos civiles y penales, Ediciones Revista General de Derecho, Valencia, 1998, pp. 87 y 88

FROSSINI, Vittorio, “La tutela de la privacidad: de la libertad informática al bien jurídico informático, en Revista del Colegio de Abogados de Buenos Aires, núm. 2, 1989, p.86

GARCÍA AMEZ, Javier, “La protección de datos del usuario de la sanidad: derecho a la intimidad y asistencia sanitaria”, en Revista Derecho y Salud, Volumen 20, Núm. 1.1, Enero – Junio, 2010, pp. 43 - 69

GARCÍA HERNÁNDEZ, Tomás Y MARZO MARTÍNEZ, B, La propiedad de la historia clínica, Edit. La Ley, 1996, p. 1629 y Ss.

GARCÍA HERNÁNDEZ, Tomás, Elementos de derecho sanitario en la responsabilidad civil y penal de los médicos por mala praxis, Edit. Edisofer, S.L., p. 85

GARCÍA HERNÁNDEZ, Tomás, Manual del médico clínico para evitar demandas judiciales, Edit. La Ley – Actualidad. Madrid, 1999, p. 84

GARRIGA DOMIGUEZ, Ana, “La protección de los datos de carácter personal en el ámbito sanitario. Usos de la historia clínica”, en GARRIGA DOMINGUEZ, Ana y ÁLVAREZ GONZÁLEZ, Susana (Dir.), Historia clínica y protección de datos Personales, especial referencia al registro obligatorio de los portadores del VIH, Dykinson S.L. 2011, pp.11 – 49.

GARRIGA DOMÍNGUEZ, Ana, Tratamientos de datos personales y derechos fundamentales, Dykinson, 2009, p.149

GIL HERNÁNDEZ, Ángel, “Protección de la intimidad corporal: aspectos penales y procesales”, en Revista General de Derecho, Valencia, Julio – Agosto, 1996, pp. 7949 - 8025

GÓMEZ CÓRDOBA, Ana I., “Consentimiento informado para el tratamiento de la información genética en el derecho colombiano”, en Revista De Derecho y Genoma Humano, Universidad de Deusto, Núm 35, Julio – Diciembre, 2011, pp.183 – 223.

GÓMEZ PIQUERAS, Cristina, “Disociación/anonimización de los datos de salud”, en Revista Derecho y Salud, Volumen 18, Número 1, Enero – Junio 2009, pp. 43 – 56.

GÓMEZ RIVERO, M^a Del Carmen, La protección penal de los datos sanitarios, especial referencia al secreto profesional médico, Edit. Comares, Año 2007, p. 85

GOMEZ RIVERO, María Del Carmen, La responsabilidad penal del médico, Edit. Tirant Lo Blanch, Valencia, 2003, p. 67

GÓMEZ SÁNCHEZ, Yolanda, “Comentario al artículo 7 – datos de salud como datos

especialmente protegidos”, en TRONCOSO REIGADA, Antonio (Dir.), Comentario a la ley orgánica de protección de datos de carácter personal, Civitas, 2010, pp. 647 – 670.

GÓMEZ SÁNCHEZ, Yolanda, “La protección de los datos genéticos: el derecho a la autodeterminación informativa”, en Revista Derecho y Salud, Volumen 16, XVI Congreso “Derecho y Salud”, 2001, pp. 59 – 78

GONZÁLEZ RUS, Juan, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en COBO DEL ROSAL, Manuel (Coord.), Derecho Penal Español – Parte Especial, Edit. Dykinson SL, 2004, Madrid, pp. 341 - 388

GRACIA, Diego, “La confidencialidad de los datos clínicos”, en CALCEDO O. Alfredo (Editor), Secreto médico y protección de los datos sanitarios en la práctica psiquiátrica, Madrid, Edit. Médica Panamericana, 2000, pp. 19 – 33

GUICHOT, Emilio, Datos personales y Administración Pública, Thomson Civitas, 2005, p.37

HEREDERO HIGUERAS, Manuel, “La protección de datos de salud informatizados en la ley orgánica 5/1992, de 29 de octubre”, en Revista Derecho y Salud, Volumen 2, Número 1, Enero Junio, 1994, pp. 17 - 28

HEREDERO HIGUERAS, Manuel, “La sentencia del tribunal constitucional de la república federal alemana relativa al censo de población de 1983”. Documentación Administrativa, N.º 198, Pp. 139-158.

HEREDERO HIGUERAS, Manuel, La ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, comentarios y textos, Edit. Tecnos, 1996, P. 76

HERRAN ORTIZ, Ana I, El derecho a la protección de datos personales en la sociedad de la información, Edit. Universidad de Deusto, Bilbao, 2003, p.90

HERRÁN ORTIZ, Ana I, La violación de la intimidad en la protección de datos personales, Dykinson, 1999, p.80.

HERRÁN ORTIZ. Ana I, El derecho a la intimidad en la nueva ley orgánica de protección de

datos personales, Edit. Dykinson, 2002, p. 19

HUALDE SÁNCHEZ, José Javier, “La protección post mortem de los derechos de la personalidad y la defensa de la memoria del fallecido”, en ASOCIACIÓN DE PROFESORES DE DERECHO CIVIL, Bienes de la personalidad, Editum, 2008, pp. 93 -148

Iniciativa, BOCG. Senado, III, A, 9 (A), 8 de Febrero de 2001. Retirada, BOCG. Senado, III A 9 (B), 1 de Marzo De 2001.

JORQUI AZOFRA, María, Análisis genéticos en el ámbito asistencial: reflexión ético – jurídica, Fundación BBVA, Edit. Comares, Granada, 2010, p. 220

JUANES PECES, Ángel, “Comentarios a los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en CONDE – PUMPIDO TOURÓN, Rogelio (Dir.), Comentarios al Código Penal, Edit. Bosh, Barcelona, 2007, pp. 1539 – 1578

LAIN ENTRALGO, Pedro, La historia clínica, Consejo Superior de Investigaciones Científicas, 1950, p.34

LAPORTA SANMIGUEL, Francisco J., “Algunas incógnitas del principio de autonomía personal en tratamientos médicos, en MENDOZA BUERGO, Blanca (Editora), Autonomía personal y decisiones médicas, Thompson Civitas, 2010, pp. 19 – 34

LAPORTA, Francisco, “Certeza y predecibilidad de las relaciones jurídicas”, en LAPORTA, F, RUIZ MANERO, J, RODILLA, M, Certeza y predecibilidad de las relaciones jurídicas, Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 55 – 93

LESMES SERRANO, Carlos, Et Al, La ley de protección de datos análisis y comentario de su jurisprudencia, Lex Nova, 2008, p.108

LOPEZ GARRIDO, Diego Y MARTÍN PALLÍN, José, “La informática: un riesgo incontrolado”, en Revista Vasca de Administración Pública, Núm. 20, Enero –Abril, 1998, pp. 201 - 218

LUCAS MURILLO DE LA CUEVA, Pablo, El derecho a la autodeterminación informativa la protección de los datos personales frente al uso de la informática, Tecnos, 1990, p. 108

MARTÍN DELPÓN, José Luis, “La protección de datos de carácter personal en el ámbito de las fuerzas armadas. La protección privilegiada de los datos relativos a la salud”, en Revista Española de Protección de Datos, Thomson, Nº 5, Julio – Diciembre -2008, pp.183 – 222.

MARTÍN SANJUÁN, Cristina, Cribado Genético: El conflicto entre el derecho a la información y el derecho a la intimidad, en MARTÍNEZ MORÁN, Narciso (Coord.), Biotecnología, derecho y dignidad humana, Edit. Comares, Granada, 2003, pp. 307 - 333

MARTINEZ CALCERRADA, Ricardo, Derecho médico – tratado de derecho sanitario, Tomo 1, Asociación Española de Derecho Sanitario, 2001, p. 773

MARTÍNEZ MARTÍNEZ, Ricard, Una aproximación crítica a la autodeterminación informativa, Civitas, 2004,P. 296

MARTÍNEZ MORÁN, Narciso, “Persona dignidad humana e investigaciones médica”, en MARTÍNEZ MORÁN, Narciso (Coord.), Biotecnología, derecho y dignidad humana, Edit. Comares, Granada, 2003, Pp.3 – 44

MAURACH, Reinhart, Tratado de Derecho Penal, Edit. Ariel, Barcelona, 1962, p. 274

MÉJICA GARCÍA, Juan M., La historia clínica: estatuto básico y propuesta de regulación, Edit. Edisofer SI, 2002, p. 16

MESSIA DE LA CERDA BALLESTEROS, Jesús A. La cesión o comunicación de datos de carácter personal, Thomson, Madrid, 2003, p. 42

MESSIA DE LA CERDA BALLESTEROS, Jesús A., La protección de datos de carácter personal en la telecomunicaciones, Universidad Rey Juan Carlos, Madrid, 2004, p.87

MICHAVILLA N, José, “El derecho al secreto profesional y el artículo 24 de la constitución. Una visión unitaria de la institución”, en Estudios sobre la Constitución Española, Tomo II; Edit. Civitas, Madrid, 1991, pp.1415 – 1436

MORALES PRATS, Fermín, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en QUINTERO OLIVARES, Gonzalo (Dir.), comentarios a la

parte especial del derecho penal, 5 Edición, Edit. Aranzadi, 2008, Navarra, pp. 401 – 466

MORALES PRATS, Fermín, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, en QUINTERO OLIVARES, Gonzalo (Dir.), Comentarios a la parte especial del derecho penal, 8 Edición, Edit. Aranzadi, 2009, Navarra, p. 404

MUNAR B, Pedro A (Et Al), Enciclopedia jurídica básica, Vol. III, Edit. Civitas S. A, año 1995, p.3725

MUÑOS CONDE, Francisco, “Falsedad documental y secreto profesional en el ámbito sanitario”, Revista Derecho y Salud, Volumen 4, Número 2, 1996, pp. 147 – 155

MUÑOZ CONDE, Francisco, Derecho Penal – Parte Especial, Edit. Tirant Lo Blanch, Valencia, 2004, p. 256

MURILLO DE LA CUEVA, Pablo L., “El derecho fundamental a la protección de los datos relativos a la salud”, en RIPOL CARULLA, Santiago (Ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Marcial Pons, 2006, pp. 21 -43

MURILLO DE LA CUEVA, Pablo Lucas, “Comentario al objeto (artículo 1 de la LOPD 15/1999)”, en TONCOSO REIGADA, Antonio (Dir.), Comentario a la ley orgánica de protección de datos de carácter personal, Civitas, 2010, pp. 75 – 96

NAVAS CASTILLO, Florentina, “Libertad de expresión y derecho a la información”, en TORRES DEL MORAL, Antonio (Dir.), Libertades Informativas, Colex, 2009, pp. 89 - 110

NICOLÁS, Pilar, “El Concepto De Dato Médico Y Genético”, En RIPOL CARULLA, Santiago (Ed.), Estudios De Protección De Datos De Carácter Personal En El Ámbito De La Salud, Marcial Pons, 2006, Pp. 78 - 101

NUÑEZ LAGOS, Rafael, perfiles de fe pública, Instituto Nacional de Estudios Jurídicos, Madrid, 1949, p. 5

OLMO FERNANDEZ – DELGADO, Leopoldo, “Estudio histórico del delito de descubrimiento y revelación de secretos”, en Revista Aranzadi de Derecho y Proceso Penal, Edit. Aranzadi, Año 2009 – 2, Número 22, pp. 111 - 130

OLMO FERNANDEZ – DELGADO, Leopoldo, El descubrimiento y revelación de secretos documentales y de las telecomunicaciones, estudio del artículo 197.1 del Código Penal, Edit. Dykinson S.L., Año 2009, p.17

ORDÓÑEZ SOLIS, David, Privacidad y protección judicial de los datos personales, Bosh, 2011.

OROSCO PARDO, Guillermo, “Protección de datos personales en el ámbito registral”, en ALVAREZ-SALA WALTHER, Juan, Et Al, Derecho de la empresa y protección de datos, Aranzadi, 2008, pp.120- 146

ORTI VALLEJO, Antonio, Derecho a la intimidad e informática (tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada), Edit. Comares, p.164

ORTS BERENGUER, Enrique y GONZÁLEZ CUSSAC, José, Compendio de derecho penal (Parte General y Especial), Edit. Tirant Lo Blanch, Valencia, 2004, p. 490

OTERO GONZÁLEZ, M^a Del Pilar, La revelación del secreto de Estado, en los procedimientos penales, Edit. Tirant Lo Blanch, Valencia 2000, p.22

PALOMAR OLMEDA, Alberto, “Confidencialidad y protección de datos en la ley de salud sexual y reproductiva y de interrupción voluntaria del embarazo, cuatro estudios”, en Revista Derecho y Salud, Volumen 20, Núm. 2, Julio – Diciembre, 2010, pp. 65 – 89

PARDO FALCÓN, Javier, “Los derechos al honor, a la intimidad personal y familiar y a la propia imagen”, en CASAS BAAMONDE, María y RODRÍGUEZ PIÑERO Y BRAVO –FERRER, Miguel, Comentarios a La Constitución Española, Año 2008, pp. 414 – 429

PEDROSA ALQUÉZAR, Sonia I., La vigilancia de la salud en el ámbito laboral, CES (Consejo Económico Social, Madrid), 2005, p. 121

PEMAN GAVÍN, Juan María, Asistencia sanitaria y sistema nacional de salud, Edit. Comares, Granada, 2005, p.309.

PEREZ – LUÑO, Antonio E., “Nuevos derechos fundamentales de la era tecnológica: libertad informática, Anuario de Derecho Público y Estudios Políticos, Núm. 2.1989 – 1990, P. 176

PEREZ – LUÑO, Antonio, “La libertad informática. Nueva frontera de los derechos fundamentales”, en Libertad informática y leyes de protección de datos personales, Cuadernos y Debates, Num.21, 1989, Pp. 133 – 213

PÉREZ DE VELASCO, José Ramón, “Protección de datos de carácter personal”, REDI, Núm. 27, 2000, p. 5

PIÑAR MAÑAS, José Luis, “Comentario al artículo 3 – concepto de dato de carácter personal”, en TRONCOSO REIGADA, Antonio (Dir.), Comentario a la ley orgánica de protección de datos de carácter personal, Civitas, 2010, Pp.184 -213

RALLO LOMBARTE, Artemi, “Uno de los principales retos en la actualidad es dar respuesta preventiva y no sólo represiva a la protección de datos personales”, en Revista Lex Nova, Abril – Junio, Número 52, 2008, pp. 8 - 10

REBOLLO DELGADO, Lucrecio, “El derecho a la intimidad”, en TORRES DEL MORAL, Antonio (Dir.), Libertades informativas, Colex, 2009, pp. 241 - 294

REBOLLO VARGAS, Rafael, La revelación de secretos e informaciones por funcionario público, Edit. Cedecs, 1996, Barcelona, pp. 138 – 139

REQUEJO NAVEROS, Teresa, “El secreto profesional del médico y su protección jurídico penal: una perspectiva histórica”, en Foro – Revista de Ciencias Jurídicas y Sociales Nueva Época, Facultad De Derecho, Universidad Complutense de Madrid, Edit. Marcial Pons, Número 6, Año 2007, Pp. 160 – 194

RIPOL CARULLA, Santiago(Ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Marcial Pons, 2006, p. 12

RODRÍGUEZ ESCANCIANO, Susana, El derecho a la protección de datos personales de los trabajadores nuevas perspectivas, Bomarzo, 2009, p. 28

RUBI NAVARRETE, Jesús, “Experiencia y criterios de la Agencia Española de Protección de Datos (AEPD), sobre los datos personales de la salud”, en RIPOLL CARULLA, Santiago (Ed.), Estudios de protección de datos de carácter personal en el ámbito de la salud, Agencia Catalana de Protección de Datos, Ediciones Jurídicas y Sociales S.A., 2006, pp.259-291

RUIZ CARRILLO, Antonio, Manual práctico de protección de datos, Bosh, 2005, p. 27

RUIZ FEGER, Andrés, “Apuntes sobre la responsabilidad civil profesional en el sector sanitario”, en Revista Española de Seguros, Editorial Española de Seguros S.L., Enero-Junio, Números 113 – 114, 2003, pp. 119 - 132

SAMPRÓN LÓPEZ, David, Los derechos del paciente a través de la información y la historia clínica, Edit. Edisofer S.L., p. 59

SÁNCHEZ CARAZO, Carmen, La intimidad y el secreto médico, Edit. Díaz De Santos, 2000, Prólogo, P. XV.

SÁNCHEZ CARO, Jesús Y SÁNCHEZ CARO, Javier, El médico y la intimidad, Edit. Díaz De Santos, 2001, Madrid, p.3

SÁNCHEZ MELGAR, Julián (Coord.), Código Penal – Comentarios y Jurisprudencia, Edit. Sepín, 2004, P. 1090

SÁNCHEZ NAVARRO, Álvaro, “La articulación del derecho a la protección de datos de carácter personal en la gestión electrónica de los procedimientos administrativos”, en Revista Española de Protección de Datos, Thomson Civitas, Julio –Diciembre, 2007, Núm. 3, pp. 95 – 169

SÁNCHEZ PATRÓN, José M, “El régimen jurídico europeo aplicable a la confidencialidad de los datos relativos a la salud de las personas”, En TOMÁS – VALIENTE L, Carmen (Coord.), La salud intimidad y libertades personales, Valencia, 2006, pp. 209 - 276

SÁNCHEZ STEWART, Nielson, “Aún quedan trincheras (algo sobre el secreto profesional y a prevención del blanqueo de capitales”, en Revista Miramar, Revista del Ilustre Colegio de Abogados de Málaga, Noviembre/Diciembre, 2007, Número 168, pp. 8 - 9

SEGRELLES DE ARENAZA, Iñigo, “Delitos contra la intimidad”, COBO DEL ROSAL, Manuel (Dir.), Compendio de derecho penal español, Edit. Marcial Pons, 2000, pp. 269 – 322

SEMPERE NAVARRO, Antonio y SAN MARTÍN MAZZUCCONI, Carolina, “Intimidad del trabajador y registros informáticos”, e ÁLVAREZ CONDE, Enrique, Revista Europea de Derechos Fundamentales, Edit. Tirant Lo Blanch, Número 1, Semestre 2003, pp. 39 - 70

SEOANE RODRÍGUEZ, José A., “¿A quién pertenece la historia clínica?”, en Revista de Derecho y Salud, Volumen 10, Número 2, Julio – Diciembre 2002, pp.231 - 254

SERRANO GÓMEZ, Alfonso y SERRANO MAÍLLO, Alfonso, Derecho Penal – Parte Especial, Edit. Dykinson, Madrid, 2009, p. 276

STARCK, Christian, En “La dignidad del hombre como garantía constitucional, en especial en el derecho alemán”, Publicado por FERNANDEZ S., Francisco (Coord.), Dignidad de la persona, derechos fundamentales, justicia constitucional, Edit. Dykinson S.L., 2008, pp. 239 - 302

SUBIZA PÉREZ, Ignacio, “La construcción del derecho a la protección de los datos personales como un derecho autónomo, en SUBIZA PÉREZ, Ignacio (Coord.), La protección de datos y sus mundos, publicaciones jurídicas, 2009, pp. 25 – 60

TIERNEY, Lawrence M Jr. / HENDERSON, Marck C., Historia clínica del paciente, método basado en evidencias, Edit. Mc Graw Hill, 2005, p. 3

TOLOSA ASENJO, Miguel A., “Gestión hospitalaria y protección de datos médicos”, en RIPOL CARULLA, Santiago (Ed.), estudios de protección de datos de carácter personal en el ámbito de la salud, Marcial Pons, 2006, pp. 121 – 158

TOMILLO URBINA, Jorge, “Nuevos derechos del paciente desde su condición jurídica como consumidor”, en Revista Derecho y Salud, Volumen 19, Extraordinario XVIII Congreso, pp. 43 – 54.

TRONCOSO REIGADA, Antonio, Protección de datos personales para servicios sanitarios públicos, Agencia de Protección de Datos de la Comunidad de Madrid, Thomson, 2008, p.27.

ULL PONT, Eugenio, Derecho público de la informática protección de datos de carácter persona, Universidad Nacional de Educación a Distancia, 2003, p. 120

VALENCIA MORENO, Alexander, Responsabilidad jurídica del médico y el seguro de responsabilidad médica, Instituto de Estudios Políticos e Internacionales Panamá, 1999, p. 17

VAZQUEZ JIMÉNEZ, Francisco, “Aspectos prácticos de la responsabilidad médica”, en Revista Miramar, Revista del Ilustre Colegio de Abogados de Málaga, Noviembre/Diciembre, 2007, Número 168, pp. 50 - 53

VIVES ANTÓN, Tomás, “Delitos contra el honor”, en Derecho Penal – Parte Especial 2da. Edición, VIVES ANTÓN, T.; ORTS BERENGUER, E.; CARBONELL MATEU, J.; GONZÁLEZ CUSSAC, J. Y MARTÍNEZ – BUJUAN PÉREZ, C., Edit. Tirant Lo Blanch, 2008, p. 314

VIZCAÍNO CALDERÓN, Miguel, Comentarios a la ley orgánica de protección de datos de carácter personal, Civitas, 2001, p.196

INFORMES Y RESOLUCIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS CITADOS

Agencia de Protección de Datos, Informe Jurídico 0156-2010

Agencia de Protección de Datos, Informe Jurídico 0593 -2009

Agencia de Protección de Datos, Informe Jurídico 2000

Agencia de Protección de Datos, Informe Jurídico 0008 - 2010

Agencia de Protección de Datos, Informe Jurídico 0020 - 2007

Agencia de Protección de Datos, Informe Jurídico 0021 – 2009

Agencia de Protección de Datos, Informe Jurídico 0046 – 2010

Agencia de Protección de Datos, Informe Jurídico 0049 - 2005

Agencia de Protección de Datos, Informe Jurídico 0061 - 2008.

Agencia de Protección de Datos, Informe Jurídico 0090 – 2009

Agencia de Protección de Datos, Informe Jurídico 0175 – 2010

Agencia de Protección de Datos, Informe Jurídico 0183 – 2009

Agencia de Protección de Datos, Informe Jurídico 0189 -2003

Agencia de Protección de Datos, Informe Jurídico 0194-2009

Agencia de Protección de Datos, Informe Jurídico 0206 - 2010

Agencia de Protección de Datos, Informe Jurídico 0242-2010

Agencia de Protección de Datos, Informe Jurídico 0266 – 2006

Agencia de Protección de Datos, Informe Jurídico 0339 - 2008

Agencia de Protección de Datos, Informe Jurídico 0340 – 2010

Agencia de Protección de Datos, Informe Jurídico 0361-2010

Agencia de Protección de Datos, Informe Jurídico 0368 – 2003

Agencia de Protección de Datos, Informe Jurídico 0382 – 2009

Agencia de Protección de Datos, Informe Jurídico 0409 – 2004

Agencia de Protección de Datos, Informe Jurídico 0410-2010

Agencia de Protección de Datos, Informe Jurídico 0494- 2009

Agencia de Protección de Datos, Informe Jurídico 0501 – 2009

Agencia de Protección de Datos, Informe Jurídico 0519 – 2009

Agencia de Protección de Datos, Informe Jurídico 0572 – 2009

Agencia de Protección de Datos, Informe Jurídico 0584 – 2009

Agencia de Protección de Datos, Informe Jurídico 0593 - 2009

Agencia de Protección de Datos, Informe Jurídico 0600 - 2009

Agencia de Protección de Datos, Informe Jurídico 0623 – 2009

Agencia de Protección de Datos, Informe Jurídico 11-2007

Agencia de Protección de Datos, Informe Jurídico 182 - 2004

Agencia de Protección de Datos, Informe Jurídico 1999

Agencia de Protección de Datos, Informe Jurídico 36 - 2004

Agencia de Protección de Datos, Informe Jurídico de 1999

Agencia de Protección de Datos, Informe Jurídico, 0167 - 2005

Agencia de Protección de Datos, Informe Jurídico, 0325 – 2009

Agencia de Protección de Datos, Informe Jurídico, 0471 - 2008

Agencia de Protección de Datos, Informe Jurídico, 0504 – 2009

Agencia de Protección de Datos, Informe Jurídico, 0511 – 2009

Agencia de Protección de Datos, Instrucción 1/1995, De 1 De Marzo

Agencia de Protección de Datos, Instrucción 2/1995, De 4 De Mayo

Agencia de Protección de Datos, Protección De Datos Personales Para Servicios Sanitarios Públicos, Edit. Agencia De Protección De Datos De La Comunidad De Madrid, 2008, Madrid,

Agencia Española de Protección de Datos, Resolución R/02182/2010, De 30 De Diciembre De 2010

SENTENCIAS CITADAS

AAP de Islas Baleares, 88 -2007, de 19 de junio de 2007.

AAP de Álava, 268-2005, de 28 de noviembre de 2005.

AAP de Barcelona, de 24 de enero de 2000.

AAP de Barcelona, de 25 septiembre de 2002.

AAP de Córdoba, de 22 de julio de 1999.

AAP de Córdoba, de 22 de julio de 1999.

AAP de Madrid, 116-2008, 5 de junio de 2008.

AAP de Madrid, 32-2002, de 11 enero de 2002.

AAP de Madrid, 413-2007, de 29 de junio de 2007.

AAP de Madrid, 498-2003, de 18 de junio de 2003.

AAP de Madrid, 56-2005, de 3 de marzo de 2005.

AAP de Pontevedra, 49-2006, de 9 de febrero de 2006.

AAP de Sevilla, 162-2006, de 18 de abril de 2006.

ATC, 600-1989, de 11 de diciembre de 1989.

ATS, de 21 abril de 2009.

ATSJ de Valencia, 10-1999, de 18 de febrero de 1999.

SAN, de 22 junio de 2005.

SAN, de 3 febrero de 2011.

SAN, de 10 octubre 2007.

SAN, de 11 febrero de 2010.

SAN, de 12 de noviembre de 2008.

SAN, de 15 de junio de 2006.

SAN, de 16 de enero de 2008.

SAN, de 16 de octubre de 2003.
SAN, de 17 de febrero de 2011.
SAN, de 17 de julio de 2006.
SAN, de 19 de noviembre de 2008.
SAN, de 19 de octubre de 2006.
SAN, de 1 de diciembre de 2009.
SAN, de 2 marzo de 2006.
SAN, de 20 de febrero de 2008.
SAN, de 20 de octubre de 2011
SAN, de 20 de septiembre de 2002.
SAN, de 21 de septiembre de 2005.
SAN, de 22 de julio de 2010.
SAN, de 22 de octubre de 2010.
SAN, de 23 de enero de 2008.
SAN, de 23 de noviembre de 2006.
SAN, de 24 de octubre de 2007.
SAN, de 24 de junio de 2010.
SAN, de 29 de abril de 2011.
SAN, de 29 de junio de 2005.
SAN, de 29 de marzo de 2006.
SAN, de 30 de mayo de 2007.
SAN, de 30 de noviembre de 2010.
SAN, de 31 de enero de 2003.
SAN, de 31 de enero de 2008.
SAN, de 8 de octubre de 2008.
SAN, de 9 de noviembre de 2005.
SAN, de 9 de octubre de 2009.
SAP de Asturias, 225-2000, de 9 de mayo de 2000.
SAP de Ávila, 57-2009, de 1 de abril de 2009.
SAP de Badajoz, 106-2002, de 16 de mayo de 2002.
SAP de Barcelona, 586-2004, de 13 de diciembre de 2004.
SAP de Barcelona, de 20 de septiembre de 2002.
SAP de Cádiz, 10-2006, 17 de enero de 2006.
SAP de Guadalajara, 138-2008, 10 de noviembre de 2008.
SAP de las Islas Baleares, 11-2009, 11 de febrero de 2009.
SAP de Las Palmas, 431-2005, de 12 de septiembre de 2005.

SAP de las Palmas, 147-2001, de 12 de noviembre de 2001.
SAP de Las Palmas, 268-2003, de 22 de abril de 2003.
SAP de Madrid, 83-2003, de 29 de enero de 2003.
SAP de Madrid, 115-1999, de 15 de abril de 1999.
SAP de Madrid, de 3 de marzo de 2003
SAP de Málaga, 11-2004, de 5 de marzo de 2004.
SAP de Pontevedra, 478-2002, de 31 de diciembre de 2002.
SAP de Santa Cruz de Tenerife, 1322-2004, de 29 de octubre de 2004.
SAP de Sevilla, 72-2002, de 15 de febrero de 2002.
SAP de Sevilla, 404-2007, de 25 de septiembre de 2007.
SAP de Teruel, 4-2002, de 6 de mayo de 2002.
SAP de Valencia, 526 – 2006, de 6 septiembre de 2006.
SAP de Vizcaya, 461 – 2000, de 18 mayo de 2000.
SJP de Palma de Mallorca, 71-2001, de 14 de marzo de 2001.
STC, 11 – 1998, de 13 de enero de 1998.
STC, 114-1984, de 29 de noviembre de 1984.
STC, 127-2003, de 30 de junio de 2003.
STC, 13-1985 de 31 de enero de 1985.
STC, 137-1985 de 17 de octubre de 1985.
STC, 156-2001, de 2 de julio de 2001.
STC, 158 – 2009, de 29 junio de 2009.
STC, 172 – 1990, 12 de noviembre de 1990.
STC, 196-2004, de 15 noviembre de 2004.
STC, 231-1988, de 2 de diciembre 1988.
STC, 254 – 1993, de 20 julio de 1993.
STC, 37-1989, de 15 de febrero de 1989.
STC, 70- 2009, de 23 marzo de 2009.
STC, 83-2002, de 22 de abril de 2002.
STC, 99 – 1994, de 11 abril de 1994.
STC, de 14 diciembre de 2005.
STS de Asturias, 2760 – 2010, de 15 noviembre de 2010.
STS, 417-2002, de 18 de febrero de 2002.
STS, 701-2000, de 25 de abril de 2000.
STS, 84-2006, de 14 de febrero de 2006.
STS, 1120 – 2008, de 19 noviembre de 2008.
STS, 1197-2007, de 23 de noviembre de 2007.

STS, 1251 – 2009, de 10 diciembre de 2009.
STS, 1288-2002, de 23 de diciembre de 2002.
STS, 1328-2009, de 30 de diciembre de 2009.
STS, 234 – 1999, de 18 febrero de 1999.
STS, 308-2001, de 26 de febrero de 2001.
STS, 574-2001, de 4 de abril de 2001.
STS, 725-2004, 11, de junio de 2004.
STS, 743- 2008, de 28 de noviembre de 2008.
STS, de 10 junio de 2011.
STS, de 11 marzo de 2011.
STS, de 17 abril de 2007.
STS, de 2 de julio de 1991.
STS, de 20 de octubre de 2009.
STS, de 20 febrero de 2007.
STS, de 23 de octubre de 2007.
STS, de 25 de febrero de 2002.
STS, de 27 mayo de 2011.
STS, de 3 diciembre de 2002.
STSJ de Andalucía, 1657 – 2008, de 12 mayo de 2008.
STSJ de Aragón, 540 - 2010, de 14 julio de 2010.
STSJ de Asturias, 1165 – 2008, de 30 septiembre de 2008.
STSJ de Asturias, 1333 – 2005, de 12 septiembre de 2005.
STSJ de Asturias, 630-2000, de 5 de junio de 2000.
STSJ de Extremadura, 932 – 2002, de 25 noviembre de 2002.
STSJ de Galicia, 438-1999, de 5 de mayo de 1999.
STSJ de Galicia, 5 – 2008, de 16 enero de 2008.
STSJ de Galicia, 5-2008, de 16 de enero de 2008.
STSJ de Galicia, 614 – 2008, de 1 octubre de 2008.
STSJ de La Rioja, de 11 de marzo de 1996.
STSJ de Madrid, 757 – 2000, de 12 julio de 2008.
STSJ de Madrid, 939-2000, de 14 de junio de 2000.
STSJ de Murcia, 208-2009, de 13 de marzo.
STSJ, de 13 de diciembre de 1996.

REFERENCIAS DE INTERNET

http://www.madrid.org/cs/Satellite?c=PAPD_Generico_FA&cid=1142660358206&language=es&pageid=1247227049247&pagename=PortalAPDCM%2FPAPD_Generico_FA%2FPAPD_fichaResolucion&vest=1247227049247, fecha de la consulta 30 de enero de 2012, hora 11:20 a.m.

Vid. El hospital Vall d'Hebron de Barcelona realiza el tercer trasplante de cara en España, (en línea), El país, 29/03/2010, http://www.elpais.com/articulo/sociedad/hospital/Vall/d/Hebron/Barcelona/realiza/tercer/trasplante/cara/Espana/elpepusoc/20100329elpepusoc_10/Tes

VALLÉS. PALMA, Matías, La sentencia que ha alarmado a la clase médica balear, (en línea), [diariodemallorca.es, 1/3/2009](http://www.diariodemallorca.es/1/3/2009), http://www.diariodemallorca.es/secciones/noticia.jsp?pRef=2009030100_2_440525__MALLORCA-sentencia-alarmado-clase-medica-balear

MAZÓN RAMOS, Pilar y CARNICERO JIMÉNEZ DE AZCÁRATE, Javier, “La informatización de la documentación clínica: oportunidad de mejora de la práctica clínica y riesgos para la seguridad y confidencialidad (en línea)”, localizable en <http://www.seis.es/documentos/informes/secciones/adjunto1/1MazonCarnicero.pdf>

Vid. Los riojanos pueden acceder a su historia clínica en Internet si disponen de certificado digital o DNI electrónico (en línea), Europapress.es, 25/11/2009, <http://www.europapress.es/la-rioja/noticia-riojanos-pueden-acceder-historia-clinica-internet-si-disponen-certificado-digital-dni-electronico-20091125131945.html>

Localizable en <http://www.20minutos.es/noticia/1497289/0/bruselas/dni-electronico/europa/>, fecha de consulta 4 de junio de 2012, 1:23 pm

Tal cual aparece publicado en el diario electrónico, el mundo.es, de fecha 19 de abril de 2009, localizable en el enlace http://www.elmundo.es/elmundo/2009/04/19/andalucia_sevilla/1240164032.html

WAGNER GRAU, Patrick, El secreto profesional o la discreción del médico (en línea), Simposio de la Academia Nacional de Medicina, año 2006 (en línea), en

http://www.acadnacmedicina.org.pe/publicaciones/Anales_2006/simposio_secreto_profesional_wagner.pdf