SESPAS
Sociedad Española de Salud Pública y Administración Sanitaria

PROTECCIÓN DE DATOS PERSONALES Y SECRETO PROFESIONAL EN EL ÁMBITO DE LA SALUD: UNA PROPUESTA NORMATIVA DE ADAPTACIÓN AL RGPD

Juan Luis Beltrán Aguirre*
Fernando José García López**
Carmen Navarro Sánchez**

Barcelona: Sociedad Española de Salud Publica y Administración Sanitaria
Noviembre de 2017

* *en representación de SESPAS*
** *en representación del Grupo de Confidencialidad y Protección de Datos de la Sociedad Española de Epidemiología*

SESPAS
Sociedad Española de Salud Pública y Administración Sanitaria

SUMARIO:

PROTECCIÓN DE DATOS PERSONALES Y SECRETO PROFESIONAL EN EL ÁMBITO DE LA SALUD: UNA PROPUESTA NORMATIVA DE ADAPTACIÓN AL RGPD

I. JUSTIFICACIÓN DE ESTE INFORME.

En el Diario Oficial de la Unión Europea de 4 de mayo de 2016 se publicó el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), que deroga y sustituye a la Directiva 95/46/CE (Comunidad Europea). Este Reglamento dispone un periodo transitorio de dos años para su entrada en vigor -establece su artículo 99 que será aplicable a partir del 25 de mayo de 2018-; periodo habilitado para que los órganos de la Unión Europea (UE) y los Estados miembros vayan desarrollando los elementos y herramientas de interpretación necesarias sobre las novedades que contiene a fin de facilitar su aplicación práctica y directa, y para que los legisladores y gobiernos de los Estados miembros procedan a la derogación y/o adaptación al RGPD de las leyes y reglamentos nacionales sobre protección de datos personales vigentes en la actualidad.

A partir del 25 de mayo de 2018, el RGPD será directamente aplicable y la primera consecuencia del principio de primacía que preside este tipo de norma europea es la inaplicación -no derogación- del derecho nacional contrario, de modo que la norma interna incompatible anterior no se aplicará y la norma interna incompatible posterior nacerá viciada por lo que tampoco debería ser aplicada. Por tanto, en el tiempo que

queda hasta mayo de 2018 ha de hacerse una exhaustiva labor de revisión de nuestra legislación para, de un lado, derogar toda aquella que resulte incompatible con el RGPD, y de otro, hacer el desarrollo y complementación normativa a que directamente habilita el propio RGPD.

De nuestra vigente normativa, a los efectos de la materia que nos ocupa, cabe destacar la Ley 41/2002, de 14 de noviembre, Básica de Autonomía del Paciente (LBAP) y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD). Pero conviene significar la falta de armonía entre ambas. La primera contempla una relación clínica en la que el protagonismo lo tiene la continuada información, oral o escrita, al paciente y la recopilación y tratamiento de la información obtenida en aras de la mejor asistencia posible. La segunda sitúa la información obtenida sobre la salud de las personas en el nivel máximo de discreción y protección[1]. En cuanto a la protección de los datos de salud, ambas leyes se hacen remisiones mutuas, lo que ha generado lagunas en su regulación. La literal aplicación de ambas leyes en ocasiones puede llevar a actos irregulares según la ley desde la que se analiza el acto en cuestión.[2]

Respecto de la remisión plena que hace el artículo 8 de la LOPD a la legislación estatal o autonómica de sanidad, ÁLVAREZ-CIENFUEGOS SUÁREZ[3], comentando este artículo en el año 2001, afirmó que la referencia genérica a la legislación sanitaria autonómica o estatal que realiza, constituía una clara insuficiencia de la Ley para contemplar las complejas garantías exigidas por el tratamiento de los datos relativos a la salud, por lo que aconsejó la aprobación de una norma específica. Posteriormente al año 2001 se han aprobado normas sanitarias que incorporan determinaciones sobre protección de datos (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 -LBAP-; Ley 16/2002, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud -LCCSNS-; Ley 14/2007, de 3 de julio, de Investigación biomédica -LIB-; Ley 33/2011, de 4 de octubre, General de Salud Pública -LGSP-, Real Decreto 1090/2015, de 4 de diciembre, que aprueba el reglamento de ensayos clínicos con medicamentos, así como diversas leyes autonómicas), pero está afirmación hoy sigue siendo válida pues tales determinaciones legales son insuficientes para presuponer que disponemos de un régimen normativo básico bastante y actualizado de protección de datos de salud que complemente el RGPD.

El Ministerio de Justicia elaboró a nivel de anteproyecto (junio de 2017) el texto de una nueva Ley Orgánica de Protección de Datos adaptada al RGPD. El Consejo de Ministros, en sesión de 10 de noviembre de 2017, lo aprobó como proyecto y lo remitió

[1] Sobre los conflictos que pueden surgir en la aplicación al mismo hecho de las dos normas, GALLEGO RIESTRA, S., "Historia clínica electrónica y derecho a la autonomía del paciente: un conflicto de intereses", en *Papeles Médicos,* vol. 23, núm. 1, 2014, pp. 7-29.

[2] Por ejemplo, se infringe la LOPD cuando se cita a un paciente por teléfono, acto que, por el contrario, encaja plenamente en la LBAP.

[3] «La aplicación de la firma electrónica y la protección de datos de la salud», en *Actualidad Informática Aranzad*i, núm. 39, 2001, p. 4

a las Cortes Generales[4]. El proyecto de dicha Ley Orgánica dispone lo siguiente en lo que hace a datos de salud:

Siguiendo el criterio del RGPD, el artículo 3 excluye la aplicación de la Ley Orgánica a los tratamientos de datos de personas fallecidas, y respecto de las personas físicas vivas

> Artículo 9. Categorías especiales de datos.
> (…)
> 2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2. del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.
>
> En particular, la ley podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro de que el afectado sea parte.

Este artículo permite, bajo la debida cobertura legal, el tratamiento de los datos biométricos, genéticos y de salud en los supuestos y marco establecidos en el artículo 9.2 del RGPD, y remite la regulación de dicho tratamiento a una ley específica en la que deberán establecerse las debidas garantías[5]. Se abstiene, pues, como lo hace la vigente LOPD, de incorporar determinaciones, disposiciones o mandatos sobre datos de salud.

Por tanto, es ineludible la necesidad de disponer de una ley específica sobre protección de datos personales relativos a la salud; ley que, por ende, se enmarcaría en la normativa del sector sanitario[6]. Hoy es opinión generalizada que lo más operativo es elaborar una ley estatal para la protección de los datos personales de salud, que complemente el RGPD y sustituya a las disposiciones contenidas en la todavía vigente LOPD, en la LBAP, y en el resto de legislación sanitaria estatal, a las que haremos puntual referencia a lo largo del presente estudio. Ello nos impulsa a elaborar este trabajo, no exclusivamente desde un planteamiento teórico-doctrinal, sino, dando un paso más, esbozando concretas propuestas de *lege ferenda* de las cuestiones a regular, acompañadas todas ellas de los correspondientes comentarios exegéticos en un intento de justificarlas, con la modesta pretensión de que puedan ayudar a la elaboración de esa ley específica tan necesaria.

---

[4] Boletín Oficial de las Cortes Generales, Serie A, núm. 13-1, de 24 de noviembre de 2017.

[5] El anteproyecto de Ley Orgánica incorporaba la disposición adicional novena en la que mandaba al Gobierno que en el plazo de dos años desde su entrada en vigor remitiera a las Cortes Generales un proyecto de ley en el que se regulasen las condiciones adicionales y, en su caso, las limitaciones al tratamiento de datos genéticos, biométricos o relativos a la salud. Sin embargo, en el proyecto de Ley Orgánica el contenido de esta disposición adicional ha desaparecido.

[6] Véase DE MIGUEL SÁNCHEZ, N., "Principios de la protección de datos: datos especialmente protegidos. Datos de carácter personal relativos a la salud: una obligada remisión a la normativa del sector sanitario" en *Comentario a la ley Orgánica de Protección de Datos de Carácter Personal*, Civitas Ediciones, 2010, pp. 708-734.

II. PROTECCIÓN DE DATOS DE SALUD EN EL ÁMBITO DE LA SALUD PÚBLICA Y EN LA INVESTIGACIÓN.

1. Encuadramiento en el marco del RGPD.

El artículo 9.1 RGPD califica los datos de salud como una categoría especial de datos personales, prohibiendo su tratamiento como regla general[7]. No puede ser de otra manera pues los datos de salud se sitúan en la esfera más íntima de la persona, particularmente, aquellos datos que su conocimiento por otros puede menoscabar el desarrollo de la personalidad, como lo son la orientación sexual, el padecimiento de enfermedades psiquiátricas o de transmisión sexual, embarazos interrumpidos, fertilidad, ser alcohólico o ex-alcohólico, drogadicto, determinadas discapacidades, portador de VIH, etc. Su tratamiento puede provocar que el responsable o un tercero que ha accedido a los datos vulnere derechos fundamentales del titular de los datos, particularmente, el derecho a la no discriminación. De ahí que los datos de salud disfruten de un estatuto jurídico particular dada su calificación como categoría especial de dato.

El artículo 9.2 del RGPD permite, entre otros supuestos, el tratamiento de datos de salud sin consentimiento del interesado cuando (finalidad y base jurídica del tratamiento):

> 9.2.h) y 9.3: el tratamiento es necesario para fines de medicina preventiva (…) cuando sea realizado por un profesional sujeto a la obligación de secreto profesional (…) o por cualquier otra persona sujeta también a la obligación de secreto, de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.
>
> 9.2.i): el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, (…) sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.
>
> 9.2.j): el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Y el apartado 4 de ese artículo señala que:

> 4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

[7] Establece que "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física."

Por otra parte, respecto a la investigación científica, el artículo 89 establece:

> 1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.
>
> 2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

Así pues, el RGPD remite al legislador de los Estados miembros la elaboración de una normativa que regule convenientemente determinadas cuestiones atinentes al tratamiento de datos personales de salud, genéticos y biométricos en el ámbito de la medicina preventiva, la salud pública y de la investigación científica, reto que, como hemos relatado, se asume mediante la disposición adicional novena del anteproyecto de nueva LOPD. Parte de ella consistirá en precisar el alcance y contenido de conceptos jurídicos indeterminados que se contienen en el RGPD. Otra parte deberá dedicarse a complementar el RGPD con el desarrollo necesario cumplimentando las remisiones que el propio reglamento hace a los legisladores nacionales. También deberán introducirse condiciones adicionales y limitaciones al tratamiento de datos y a los derechos de los interesados en función de los intereses que nuestro legislador considere deban salvaguardarse. Finalmente, deberá regularse el secreto profesional y sus excepciones.

Toda esta normativa constituirá la base jurídica del tratamiento, de la que, junto a los fines, se debe informar puntualmente a los interesados (artículos 13 y 14 RGPD).

2. Definición de interés público en el ámbito de la salud pública.

Propuesta de regulación:

1. A los efectos del artículo 9.2.i) del Reglamento (UE) 2016/679, de 27 de abril de 2016, son de interés público en el ámbito de la salud pública las actuaciones sanitarias y los estudios epidemiológicos necesarios para la prevención de un riesgo o peligro grave e inminente para la salud de la población. Entre estas actividades se incluye la vigilancia epidemiológica de las enfermedades de declaración obligatoria y aquellas enfermedades que las autoridades sanitarias consideren necesario vigilar. Las enfermedades objeto de vigilancia epidemiológica serán determinadas por las autoridades sanitarias en las normas correspondientes.

2. La autoridad sanitaria y los órganos competentes de las Administraciones sanitarias a los que se refiere la Ley 33/2011, General de Salud Pública, podrán recabar la comunicación de datos personales en poder de cualquier Administración o de entidades privadas cuando el conocimiento de tales datos resulte necesario para el desempeño de sus funciones legítimas de tutela de la salud pública.

Comentario exegético:

El considerando 54 RGPD advierte expresamente que "*El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) nº. 1338/2008 del Parlamento Europeo y del Consejo, es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines*."

El artículo 9.2. i) del RGPD no concreta o define el sentido y alcance de la expresión "interés público", por lo que la aplicación directa del RGPD en los Estados miembros posiblemente genere diversas interpretaciones de ese concepto, de modo que finalmente serán las autoridades de control y los tribunales quienes terminen fijando su alcance. Como ejemplo de interés público en salud pública el artículo 9.2.i) del RGPD cita *la protección frente a amenazas transfronterizas graves para la salud*. Pues bien, el artículo 3.g) de la Decisión n.º 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud, define amenaza transfronteriza grave para la salud como "*una amenaza para la vida u otro grave peligro para la salud de origen biológico, químico, ambiental o desconocido que se propaga o implica un riesgo significativo de propagarse a través de las fronteras nacionales de los Estados miembros y que puede requerir coordinación a nivel de la Unión para garantizar un nivel elevado de protección de la salud humana."* Con estos antecedentes ha de entenderse que un "interés público" en el ámbito de la salud pública, a efectos de excepcionar el consentimiento del interesado, solo acoge como norma general las actuaciones y los estudios epidemiológicos y de salud pública cuya finalidad directa sea la prevención de un riesgo grave para la salud de la población (enfermedades transmisibles; control de epidemias y de su propagación; amenazas transfronterizas graves; situaciones de urgencia humanitaria por catástrofes naturales o de origen humano). Su rápida detección exige un acceso a información multidisciplinaria y una

correcta evaluación del riesgo o peligro, y la investigación en salud pública es fundamental para una adecuada respuesta ante amenazas sanitarias.[8]

Así pues, el concepto "interés público" no acoge aquellos estudios epidemiológicos cuya finalidad es poder mejorar la salud de la población (investigar causas del cáncer; la relación entre el nivel socioeconómico y una enfermedad concreta, etc.). Estos últimos, a efectos del RGPD, entrarían en el régimen diseñado para la "investigación científica" (en estos casos investigación dirigida a mejorar la salud de la población), y esta actividad científica tiene difícil encaje en el concepto jurídico "interés público" ya que no tiene como finalidad evitar, reducir o prevenir un peligro que supone una amenaza grave e inminente para la salud de la población. La actividad científica es, por supuesto, una actividad de interés general, pero no reúne las notas de imperiosidad (considerando 69), gravedad e inminencia, que identifican a un "interés público" conforme la acepción que otorga el RGPD a este sintagma. Una cosa es el concepto amplio de salud pública (considerando 54) y otra que todos los elementos que lo integran sean *per se* necesariamente de un interés público tal que justifique hacer prevalecer el concreto interés del estudio sobre los intereses, derechos y libertades de los interesados. En estos casos, para poder excepcionar el consentimiento y no enmarcar el estudio en el régimen diseñado por los artículos 9.2 j) y 89 del RGPD para la investigación científica, habrá que motivar y justificar expresamente cuál es el "interés público" subyacente en cada estudio o investigación que se programe.

3. Actuaciones de salud pública, epidemiología, protección de datos y consentimiento de los interesados.

Propuesta de regulación:

1. Los centros y servicios sanitarios públicos y privados y los profesionales sanitarios deben ceder a la autoridad sanitaria o a los órganos competentes de las Administraciones sanitarias, los datos identificativos de los pacientes que resulten imprescindibles para la toma de decisiones cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población y así se les requiera motivadamente por razones epidemiológicas o de salud pública[9].

La Administración comunicante o la entidad privada dejará constancia de la finalidad señalada por el órgano responsable en materia de salud pública y del contenido de la comunicación realizada. El órgano responsable en materia de salud pública quedará obligado, por el solo hecho de la comunicación, a la observancia de las disposiciones

[8] El artículo 12.1 de la LGSP establece que "*la vigilancia en salud pública es el conjunto de actividades destinadas a recoger, analizar, interpretar y difundir información relacionada con el estado de la salud de la población y los factores que la condicionan, con el objetivo de fundamentar las actuaciones de salud pública.*"

[9] Artículos 41 de la Ley 33/2011, de 4 de octubre, General de Salud Pública y 16.3 Ley 41/2002, de 14 de noviembre, de Autonomía del Paciente.

relativas a la protección de los datos personales en relación con los datos comunicados[10].

2. Las Administraciones sanitarias no precisarán obtener el consentimiento de los interesados a fin de recabar y almacenar sus datos personales de salud con vistas a ser tratados en la tutela de la salud pública.

En la investigación epidemiológica normalmente se trabajará con datos anonimizados o, en su caso, seudonimizados[11]*. Se podrá acceder a los datos identificativos de los pacientes por razones epidemiológicas, de protección de la salud pública y de medicina preventiva en los siguientes ámbitos: a) vigilancia de las enfermedades de declaración obligatoria, b) vigilancia de enfermedades a través de sistemas de información microbiológico; c) estudio y control de brotes; d) investigación de reacciones adversas a la vacunación y mejora del programa de vacunaciones; e) mejora de programas de cribado poblacional; e) registro de tumores y otros registros poblaciones promovidos por las autoridades administrativas; f) mejora de registro de mortalidad. El acceso queda limitado a los fines específicos de cada caso.*

3. Serán excepciones al consentimiento informado exclusivamente las previstas en normas de Derecho comunitario o en normas con rango de ley que autoricen la recogida y tratamiento de datos de salud para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias o que sean atribuidas por dichas normas.

4. Las Administraciones sanitarias velarán especialmente por el recto cumplimiento de las condiciones de seguridad en el tratamiento y conservación de los datos tratados con fines de salud pública, para lo que deberán aplicar las medidas técnicas y organizativas previstas en la legislación de protección de datos de carácter personal.

Comentario exegético:

a) Actuaciones de salud pública.

El artículo 9.2.i) del RGPD establece que es legítimo comunicar datos a la Administración sanitaria sin consentimiento previo del interesado cuando es necesario por razones de interés público en el ámbito de la salud pública. En la comunicación de datos por razones de prevención y protección de la salud de la población, conviene recordar que cuando el artículo 9.2.i) del RGPD habla de motivos de interés público en el ámbito de la salud pública como razón para excepcionar el consentimiento del interesado, el legislador europeo está pensando en la evaluación y las respuestas (que en nuestro país se instrumentarán a través de las medidas habilitadas por la Ley Orgánica 3/1986, de 14 de abril) ante amenazas para la salud pública (amenazas potenciales,

[10] Tomado del artículo 58 de la Ley 5/2014, de 26 de junio, de Salud Pública, de Aragón. En términos similares el artículo 41 de la LGSP.
[11] Codificados según la vigente normativa nacional.

crisis sanitarias, desastres naturales, etc.). Pues bien, su rápida detección exige un acceso a información múltiple y una correcta evaluación del riesgo o peligro, y la práctica de la salud pública es fundamental para una adecuada respuesta ante amenazas sanitarias[12]. En este contexto, la cesión de datos identificativos del paciente está justificada cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población. Con este mismo alcance se pronuncia el artículo 16.3 LBAP. Además, la LBAP (artículos 7 y 16) previene que el acceso quede limitado a los fines específicos de cada caso, por lo que será necesario, por tanto, aplicar criterios de estricta necesidad, idoneidad y proporcionalidad para obtener la información.[13]

b) Epidemiología.

El artículo 11 de la LCCSNS enumera las prestaciones de salud pública. Las prestaciones o actuaciones de salud pública se encuadran en lo que se ha denominado actividad rutinaria de la epidemiología. Junto a la práctica epidemiológica rutinaria se sitúan los estudios o investigación epidemiológica. Ambos campos están muy conectados por lo que no es fácil separar la práctica rutinaria epidemiológica de la investigación epidemiológica propiamente dicha[14].

La Ley 14/1986, de 25 de abril, General de Sanidad (LGS), determinó en su artículo 8.1 como actividad fundamental del sistema sanitario la realización de estudios epidemiológicos para orientar con mayor eficacia la prevención de los riesgos para la salud, actividad que debía tener como base, con la cesión de informes, protocolos, datos, etc., un sistema organizado de información sanitaria, vigilancia y acción epidemiológica.

Pues bien, para facilitar la recogida de la información necesaria a que se refiere la LGS, el art. 41 de la LGSP, dispone que

> 1. Las autoridades sanitarias con el fin de asegurar la mejor tutela de la salud de la población podrán requerir, en los términos establecidos en este artículo, a los servicios y profesionales sanitarios informes, protocolos u otros documentos con fines de información sanitaria.
> (…)
> 3. A los efectos indicados en los dos apartados anteriores, las personas públicas o privadas cederán a la autoridad sanitaria, cuando así se las requiera, los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública. En cualquier caso, el acceso a las historias clínicas por razones epidemiológicas y de salud pública se someterá a lo dispuesto en el apartado 3 del artículo 16 de la Ley 41/2002, de

[12] En el preámbulo de la LGSP se dice que "*para mejorar la calidad de las actuaciones en salud pública, estas han de estar muy ligadas a un tipo de actividad investigadora que promueva cauces de conocimiento….".*

[13] Así se pronuncia el Auto de 26 de julio de 2004 -JUR/2004/223958- de la Audiencia Provincial de Tarragona.

[14] Véase el Documento International Ethical Guidelines for Epidemiological Studies de CIOMS-OMS, disponible en: http://www.cioms.ch.publications/guidelines/1991_texts_of_guidelines_htm

14 de noviembre, básica reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica"[15].

Corresponde al Consejo Interterritorial del SNS aprobar la información que debe incluirse en el Sistema. El apartado 3 del artículo 41 de la LGSP permite, pues, el acceso a los datos identificativos del paciente sin su consentimiento solo en situaciones de riesgo grave.

Los datos de carácter personal, recogidos y elaborados por las Administraciones sanitarias para el desempeño de sus funciones, han de ser comunicados a los sistemas de información de vigilancia en salud con objeto de su posterior tratamiento para fundamentar las actuaciones de salud pública y lograr una mejor protección de la salud de los ciudadanos, así como con fines estadísticos o científicos en el ámbito de la salud pública. La información obtenida se ha de integrar en los registros de enfermedades y determinantes de salud que, a su vez, componen el Sistema de Información en Salud Pública (artículo 40 de la LGSP). Ello por cuanto contar con un buen sistema de información que pueda dar respuestas a las expectativas y necesidades de los ciudadanos y profesionales sanitarios es uno de los elementos clave para hacer frente a los retos derivados de la organización de la salud pública y de las demandas que plantean los ciudadanos, los profesionales y las Administraciones sanitarias.

El sistema de información sanitaria ha evolucionado desde los tradicionales modelos de explotación de datos independientes y descriptivos al actual sistema que permite tratar electrónicamente la información de forma integrada generando mayor conocimiento, de modo que los sistemas sanitarios pueden posicionarse ventajosamente para dar respuesta a las exigencias de la sociedad a la que sirven y sortear las eventuales amenazas biológicas. Actualmente, se dispone de avanzados indicadores sobre enfermedad, sobre asistencia sanitaria y sobre conductas relacionadas con la salud, pero no están integrados con información procedente de otros ámbitos sociales, ambientales o de otro carácter, que también son esenciales para valorar la evolución de la salud pública y las políticas con ella relacionadas. Estos registros tienen como función, precisamente, alcanzar esa integración.

---

[15] Art. 16.3. *El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.*
(...)
Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

La investigación epidemiológica estudia enfermedades y todo tipo de fenómenos relacionados con la salud[16]. Cuando el eje de la investigación son los determinantes de salud surge la epidemiología social[17]. Cuando se investiga la frecuencia y distribución de la enfermedad, sus determinantes y factores de riesgo, hablamos de epidemiología de salud pública, y cuando se aplican los principios y métodos epidemiológicos a los problemas encontrados en la medicina clínica hablamos de epidemiología clínica en la que el denominador está conformado por personas con una condición clínica particular o una enfermedad[18]. Los estudios epidemiológicos según su temporalidad se clasifican en retrospectivos, que es un estudio longitudinal en el tiempo que se analiza en el presente, pero con datos del pasado, en los que generalmente se trabaja con datos anonimizados, y en prospectivos, que es un estudio longitudinal en el tiempo que se comienza en el presente, pero los datos se analizan transcurrido un cierto tiempo, en el futuro, en los que generalmente se trabaja con datos personalizados. Según el tipo de resultado a obtener, se clasifican en descriptivos y analíticos y estos últimos en observacionales (de prevalencia) o ensayos clínicos (de intervención)[19].

En la investigación epidemiológica, no siempre es viable la anonimización o la seudonimización para realizarla con éxito. Los epidemiólogos, para realizar estudios de epidemiología social o cuya finalidad sea poder mejorar la salud de la población, esto es, sin que medie un riesgo o peligro grave para la salud de la población[20], con frecuencia también necesitan acceder a los datos de salud de pacientes identificados incluso sin su consentimiento. Ello porque, de un lado, la práctica acredita que normalmente no se obtiene más de un 45% o 50% de consentimientos (en los estudios retrospectivos muchos pacientes pueden haber muerto) y esas cifras no son suficientes

[16] El concepto de epidemiología ha evolucionado en el tiempo enfatizando en cada contexto histórico alguno de los elementos propios de esta disciplina. Así, se han identificado tres etapas: a) era de las miasmas que dura hasta mediados del siglo XIX; b) era de las enfermedades infecciosas que transcurre desde mediados del siglo XIX hasta mediados del siglo XX; c) era de las enfermedades no infecciosas crónicas, que se inicia a partir de mediados del siglo XX por causa del control de las enfermedades infecciosas (vacunaciones), lo que motiva que la epidemiología se extienda a enfermedades no infecciosas como las cardiovasculares, el cáncer, etc. VIGUERA ESTER, P., "La investigación en salud pública" en PALOMAR OLMEDA y CANTERO MARTÍNEZ (dirección)*Tratado de Derecho Sanitario,* Tomo II, Thomson Reuters Aranzadi, 2013, pp. 1072-1075.

[17] La epidemiología social investiga de manera explícita los determinantes sociales de las distribuciones de la salud, la enfermedad y el bienestar en las poblaciones, en vez de tratar dichos determinantes como un simple trasfondo de los fenómenos biomédicos. Por lo tanto, la epidemiología social pretende conocer cómo los factores sociales afectan a la salud de la población. Definición de BORRELL, C. "Epidemiología social: la persona, la población y los determinantes sociales de la salud", en *Cuadernos de la Fundación Dr. Antonio Esteve,* núm. 32, "Epidemiología para periodistas y comunicadores", 2015, p. 33. Véase también los relevantes trabajos de PUYOL, Á, "Ética, equidad y determinantes sociales de salud" en *Gaceta Sanitaria,* vol. 26, núm. 2, 2012, pp. 178-181 y "La idea de la solidaridad en la ética de la salud pública" en *Revista de Bioética y Derecho,* núm. 40, 2017, pp. 33-47.

[18] Véase BERMEJO FRAILE, B, *Epidemiología clínica aplicada a la toma de decisiones en medicina,* Gobierno de Navarra, 2001; GARCÍA GARCÍA, J. J. "Epidemiología clínica. Qué y para qué" en *Revista Mexicana de Pediatría,* vol. 66, núm. 4, 1999, pp. 169-173.

[19] Véase GÓMEZ PIQUERAS, C., "Disociación/anonimización de los datos de salud" en *Derecho y Salud*, vol. 18, núm. 1, 2009, p. 53.

[20] SERRANO PÉREZ, M.ª, M., pone como ejemplos el seguimiento de enfermedades raras, la diabetes infantil o el VIH, "Salud pública, epidemiología y protección de datos", en el libro colectivo PALOMAR OLMEDA y CANTERO MARTÍNEZ (dirección) *Tratado de Derecho Sanitario*, Volumen II, Thomson-Reuters-ARANZADI, 2013, p. 1105.

para las investigaciones, y, de otro lado, la anonimización no es solución pues impide investigaciones de calidad ya que la probabilidad de error con datos anónimos es bastante alta[21]. Una de las fuentes de datos para los estudios epidemiológicos y de salud es la historia clínica electrónica[22]. Los ámbitos en los que en razón de criterios técnicos o científicos epidemiológicos se requiere la identificación de la persona titular de las historias clínicas a tratar son[23]: a) vigilancia de las enfermedades de declaración obligatoria, b) vigilancia de enfermedades a través de sistemas de información microbiológica; c) estudio y control de brotes; d) investigación de reacciones adversas a la vacunación y mejora del programa de vacunaciones; e) mejora de programas de cribado poblacional; e) registro de tumores; f) mejora de registro de mortalidad. En definitiva, en los ámbitos reseñados es aconsejable trabajar con datos personalizados o, a lo sumo, seudonimizados de modo que pueda realizarse fácilmente el proceso inverso a la disociación, ya que puede ser necesario disponer de la identidad de los sujetos de la investigación y, por ende, debe ser posible acceder a dicha identidad con facilidad.

Pero en alguno de esos ámbitos reseñados no concurre un riesgo o peligro grave para la salud de la población. No obstante, en el artículo 9.2 del RGPD encontramos dos fines que habilitan a realizar estos estudios epidemiológicos sin recabar el consentimiento de los interesados: fines de medicina preventiva[24] (letra h) y fines de investigación científica (letra j). Nótese que el artículo 17.3.c) del RGPD -sobre el derecho de supresión (el derecho al olvido)- anuda las letras h) e i) a razones de interés público en el ámbito de la salud pública.

4. Concepto de investigación científica.

Propuesta de regulación:

1. A los efectos del artículo 9.2.j) del Reglamento (UE) 2016/679, de 27 de abril de 2016, es investigación científica la investigación aplicada y la epidemiológica,

[21] Al respecto, SERRANO PÉREZ, M.ª. M., SÁNCHEZ NAVARRO, C. y ZURRIAGA LLORENS, C., "A modo de reflexión y crítica en torno a la propuesta de reglamento europeo de protección de datos y algunas de las enmiendas presentadas en relación con la epidemiología y la salud", en *Derecho y Salud,* vol. 23, extraordinario, 2013, pp. 292-293.

[22] Según el art. 17.1 LBAP, la historia clínica ha de conservarse cinco años como mínimo tras el alta de cada proceso asistencial. No obstante, precisa el art. 7.2 que se conservará la historia clínica cuando existan razones epidemiológicas o de investigación, y que su tratamiento se hará de forma que se evite en lo posible la identificación del paciente.

[23] Se sigue la Orden de 26 de octubre de 2011, de Galicia, que especifica los criterios técnicos y/o científicos para el acceso a la historia clínica a efectos epidemiológicos y de salud pública (DOG de 16-11-2011).

[24] Opina DE MIGUEL SÁNCHEZ, N., que los fines de prevención médica incluyen los estudios epidemiológicos, "Investigación y protección de datos de carácter personal: una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica", en *Revista Española de Protección de Datos,* núm. 3, 2006, p. 190. Y, en efecto, la prevención médica exige disponer de estudios epidemiológicos en los que apoyar los programas preventivos. El artículo 19.1 de la LGSP establece la prevención tiene por objeto reducir la incidencia y la prevalencia de ciertas enfermedades, lesiones y discapacidades en la población y atenuar o eliminar en la medida de lo posible sus consecuencias negativas mediante políticas acordes con los objetivos de esa ley.

aprobadas y financiadas por la Administración pública e integradas en el Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica.

La investigación en salud pública y la epidemiológica se desarrollará en el marco de la Estrategia de Salud Pública.

2. También tendrá la consideración de investigación científica la investigación privada que se desarrolle en el marco del Área de Ciencias de la Vida del Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica.

3. La investigación pública y privada, además, deberá estar aprobada por el Comité de Ética de la Investigación correspondiente.

4. Las Autoridades sanitarias, en situaciones extraordinarias de excepcional relevancia y gravedad para la salud pública, podrán llevar a cabo estudios científicos sin el consentimiento de los afectados.

Comentario exegético:

El concepto de investigación biomédica comprende fundamentalmente tres maneras de hacer investigación[25]:

a) La investigación básica o preclínica, que persigue un mejor conocimiento de los mecanismos moleculares, bioquímicos y celulares implicados en la etiopatogenia de las enfermedades, a la vez que determinar la importancia de los aspectos epigenéticos en su génesis. En esta investigación se pueden utilizar datos de salud personalizados si se quiere vincular resultados de la investigación con la evolución clínica de los sujetos, en cuyo caso se emplearán muestras codificadas (pseudonimizadas). En caso contrario, cuando no son precisos los vínculos con la evolución clínica, se utilizan muestras biológicas anónimas o anonimizadas.

b) La investigación clínica, centrada en los pacientes, que estudia la prevención, diagnóstico y tratamiento de las enfermedades y el conocimiento de su historia natural. Dentro de la investigación clínica hospitalaria se pueden clasificar.
- Ensayos clínicos con medicamentos.
- Ensayos clínicos con prótesis, técnicas quirúrgicas, etc.
- Estudios retrospectivos.
- Tesis, proyectos de fin de grado, etc.

Todos ellos pueden requerir el acceso a la historia clínica para lo que es exigible el VB de Comité de Ética de Investigación del hospital.

[25] GUTIÉRREZ, J.A. y CARRASCO, M. "Gestión de investigación biomédica" en: Gutiérrez, J.A. y Puerta, J.C., editores. *Reflexiones sobre la ciencia en España. El caso particular de la biomedicina.* Madrid: Fundación Lilly, 2003; 137-66.

c) La investigación epidemiológica o en salud pública[26] tiene por objeto a la población y estudia la frecuencia y distribución de los fenómenos relacionados con la salud y sus determinantes en poblaciones específicas, sus factores de riesgo e impacto en la salud pública, así como el impacto, calidad, y costes que las acciones y recursos de los sistemas sanitarios tienen sobre la salud de la población.

Diversos textos internacionales reconocen la libertad de investigación como parte del contenido de la libertad de pensamiento y de expresión. El artículo 13 de la Carta de Derechos Fundamentales de la UE establece que "*la investigación científica es libre"*. El artículo 20 de la Constitución Española -CE- reconoce el derecho a la producción científica y el 44 ordena a los poderes públicos promover la investigación científica. Ahora bien, en el ámbito de la investigación biomédica la libertad científica ha de estar siempre supeditada a la dignidad humana y a la integridad de la persona y convenientemente enmarcada en unos principios éticos (Declaración Universal sobre Bioética y Derechos Humanos de la UNESCO de 2005). Y, en efecto, el citado artículo 20 de la CE, en su apartado 4 establece que "estas libertades tienen su límite en el respeto de los derechos reconocidos en este Título…". Buen ejemplo de ello es la Ley 14/2007, de 3 de julio, de Investigación Biomédica (LIB), reguladora de la investigación biomédica básica y aplicada que se hace en nuestro país, que se ha construido sobre los principios de la integridad de las personas y la protección de la dignidad e identidad del ser humano. Como ha apuntado ROCA TRÍAS[27] la libertad de investigación no hay que enfrentarla al derecho a la salud sino a los derechos fundamentales contenidos en la sección primera del capítulo segundo del título primero de la CE. En suma, la libertad de investigación no es un valor absoluto pues ha de acomodarse a los requisitos que establezca el ordenamiento jurídico inspirados en el respeto de la dignidad del ser humano y encaminados a prevenir y evitar los posibles riesgos de la actividad investigadora. Esa regulación, además, ha de incorporar normas de patrocinio y tutela que garanticen la independencia del investigador y la primacía de los intereses científicos sobre los económicos, a la par que establezca los debidos controles y garantías en la financiación pública[28]. A estas reglas jurídicas y éticas debe someterse la investigación científica pública y privada para tenerse como tal.

Respecto de la investigación sanitaria que pueda hacerse en nuestro país, el artículo 45 de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud, encomienda al Ministerio de Sanidad, teniendo en cuenta las propuestas que formulen las comunidades autónomas y las necesidades y objetivos que enumera el apartado tercero de dicho artículo, la elaboración de una iniciativa sectorial de

[26] Precisa el considerando 159 del RGPD que "Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública."

[27] "La función del derecho a la protección de la persona ante la biomedicina y la biotecnología", en el libro colectivo *Derecho biomédico y bioética*, editorial Comares, 1998, p.174.

[28] Véase al respecto RUÍZ LAPEÑA. R., voz "Libertad de investigación" en ROMEO CASABONA (director) *Enciclopedia de Bioderecho y Bioética,* Tomo II, Editorial Comares, S.L, 2011, pp. 1046-1055, y PELAYO GONZÁLEZ-TORRE, A., "Investigación con seres humanos: límites bioéticos y jurídicos" en PALOMAR OLMEDA y CANTERO MARTÍNEZ (dirección), *Tratado de Derecho Sanitario,* vol. II, Thomson Reuters Aranzadi, 2013, pp. 825-865.

investigación en salud que se integrará en el Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica. La Ley, que incorpora el principio de que la innovación de base científica es esencial para el desarrollo de los servicios sanitarios y para la efectiva protección de la salud de los ciudadanos, concreta las responsabilidades del Ministerio en este aspecto y le encomienda, en colaboración con las comunidades autónomas en el seno del Consejo Interterritorial del Sistema Nacional de Salud, la elaboración de la iniciativa sectorial de investigación en salud, que se incorporará al Plan Nacional de I+D+I[29], así como la designación de centros de investigación del Sistema Nacional de Salud. También encomienda al Instituto de Salud Carlos III, creado por la Ley General de Sanidad, funciones de planificación de la investigación, vertebración de los recursos dedicados a ella, difusión y transferencia de resultados y desarrollo de programas de investigación. Por su parte, la LIB establece los requisitos ético-jurídicos en los que se ha de desarrollar la investigación biomédica. Finalmente, el artículo 49 de la LGSP crea la Estrategia de Salud Pública como marco para determinar las prioridades de investigación en salud pública.

El considerando 159 del RGPD señala que "*el tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública*." Sin embargo, entendemos que es necesario diferenciar el concepto amplio de investigación que sienta el RGPD del concreto marco en el que los profesionales realizan cada investigación. En decir, para considerar una investigación acogida al régimen de excepción del consentimiento del artículo 9.2.j) del RGPD debe ser una investigación institucional, no a nivel personal. El Informe 0073/2010 de la AEPD exige esta premisa cuando afirma que *"se desconoce si el investigador va a desarrollar el estudio a título personal o, si por el contrario, se trata de un proyecto institucional a realizar en el marco de algún programa de investigación concreto incluido en el Plan Nacional de Investigación Científica, Desarrollo e Innovación. Lo anterior es importante, a efectos de valorar si nos encontramos en presencia de un auténtico estudio científico y en consecuencia amparado por el supuesto de cesión contemplado en el artículo 11. 2 e) y 21. 1 de la Ley15/1999, cuando aluden al fin científico del tratamiento de los datos personales como supuesto que excluye el consentimiento previo a la cesión de los mismos, si el cedente y cesionario son administraciones públicas.*"

[29] En sesión celebrada el 30 de diciembre de 2016, el Consejo de Ministros aprobó la prórroga del Plan Nacional de Investigación Científica, Técnica y de Innovación 2013-2016, que estará en vigor hasta que se apruebe el futuro Plan Estatal correspondiente al período 2017-2020, en el que ya está trabajando la Secretaría de Estado de I+D+i del Ministerio de Economía, Industria y Competitividad. Pues bien, este Plan, respecto a la salud humana, diseña la siguiente estrategia.

Estos son, pues, los mimbres normativos que enmarcan la investigación científica en el área de la salud pública. Con la propuesta de regulación que hacemos, tratamos de definir y encajar la investigación científica en el ámbito marco del artículo 45 de la Ley de Cohesión y Calidad del Servicio Nacional de Salud (SNS).

5. Investigación científica, protección de datos y consentimiento de los interesados.

Propuesta de regulación:

1. Para obtener información necesaria con la que hacer investigación sanitaria y epidemiología social, con el fin de mejorar la eficacia de la prevención de los riesgos y la planificación sanitaria, las Administraciones sanitarias podrán crear registros destinados a recoger datos sobre las enfermedades y los distintos determinantes de la salud. [30]

Cuando los registros contengan ficheros donde hayan de almacenarse datos personales, su creación, modificación o supresión, deberá realizarse mediante disposición de carácter general, en la que, además de los requerimientos y exigencias derivados de la normativa de protección de datos personales, se expondrán las concretas razones de interés general sanitario que justifiquen la existencia del fichero y las finalidades perseguidas con el mismo.

2. En la investigación científica pública como regla general solo se podrá acceder para su tratamiento a los datos de salud que previamente hayan sido anonimizados o seudonimizados. Siempre que los fines de la investigación puedan alcanzarse prescindiendo de la identificación de los interesados se procederá a la anonimización de todos los datos. Siempre que los fines de la investigación puedan alcanzarse desligando la información que identifica a la persona utilizando un código que permita la operación inversa, se procederá a la seudonimización.

Sin perjuicio de lo establecido en el artículo 5.1.b) del Reglamento (UE) 2016/679, de 27 de abril de 2016, cuando sea necesario trabajar con datos personalizados será preciso recabar un nuevo y específico consentimiento del interesado para tratar los datos de salud que se recogieron inicialmente con fines asistenciales, salvo la excepción establecida en el apartado 5 de este artículo.

3. En la investigación científica solo se podrá acceder para su tratamiento a datos previamente anonimizados irreversiblemente, salvo que el propio interesado haya dado su consentimiento para no disociar sus datos identificativos de los de carácter clínico-asistencial.

4. A los efectos de los apartados anteriores los responsables de ficheros y archivos de historia clínicas electrónicas deberán disponer de un sistema informático que articule

[30] Conforme al artículo 19.2.a) de la LGSP son determinantes de salud los factores sociales, económicos, laborales, culturales, alimentarios, biológicos y ambientales que influyen en la salud de las personas.

una opción de disociación automática para cuando hayan de cederlas con fines de investigación científica.

5. En estudios de investigación científica públicos con datos personales que requieren especial protección, los comités de ética de la investigación, excepcionalmente, podrán dispensar del consentimiento de los sujetos implicados si consideran que se dan las tres condiciones siguientes:

a) que el estudio sea observacional y tenga un valor social indudable
b) que el estudio solo se pueda llevar a cabo sin anonimización y sin el consentimiento de los interesados ya que su obtención sería impracticable o excesivamente costosa.
c) que el riesgo para los sujetos participantes sea mínimo.

6. El tratamiento de datos en la investigación científica privada con ánimo de lucro requerirá un nivel de control mayor que la investigación científica pública sin ánimo de lucro. Como regla general, será necesario el consentimiento informado escrito. Las condiciones para el tratamiento de datos sin el consentimiento informado de los participantes serán más restrictivas y se determinarán por los Comités de Ética de Investigación en función del tipo y fines de la investigación.

7. Queda prohibido todo proceso dirigido a la reidentificación de las personas mediante la asociación de datos personales a datos de salud que tengan la consideración técnica y jurídica de anonimizados. La desanonimización de datos de manera que permita la reidentificación de las personas, constituye una infracción muy grave que será sancionada conforme al régimen sancionador y el procedimiento establecidos en la Ley Orgánica de Protección de Datos Personales.

Comentario exegético:

a) Registros e investigación observacional.

Respecto a la investigación científica, el considerando 157 del RGPD precisa que: *Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales.* Es, pues, evidente la importancia que el RGPD

otorga a los registros de enfermedades y determinantes de salud de cara a la investigación científica y los estudios de epidemiología de salud pública y social.

La OMS define al registro como un fichero de documentos que contienen información uniforme acerca de personas individuales, recogida de forma sistemática e integral, para que sirva a unos objetivos previamente establecidos científicos, clínicos o de política sanitaria. Se crean registros específicamente con fines de investigación. La LBAP identifica a la historia clínica como principal fuente de información que nutre los registros. La investigación con registros es observacional pues se realiza con individuos respecto de los que no se modifica el tratamiento o intervención al que está sometidos, ni se les prescribe pautas que puedan afectar a su integridad física. No hay procedimientos invasivos. De ahí que la LIB los excluya de su aplicación.

Los estudios observacionales se hacen con datos obtenidos de registros y el tratamiento de los daos se sujeta a la LBAP y a la LOPD. La investigación con procedimientos invasivos se sujeta a una legislación específica. La LIB.

b) Minimización de los datos.

El artículo 89.1 RGPD exige rotundamente la aplicación del principio de minimización en el tratamiento de datos para la investigación; principio que el artículo 5.1.c) del referido Reglamento perfila al establecer que los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que fueron tratados.

Este principio de minimización es equivalente o asimilable al principio de proporcionalidad elaborado por nuestro Tribunal Constitucional, que se integra de tres elementos: a) el de utilidad o adecuación; b) el de necesidad; c) el de proporcionalidad *strictu sensu* o ponderación de los bienes en conflicto.

En suma, no es suficiente con la anonimización o seudonimización de los datos, pues la recogida de datos por el responsable ha de limitarse a aquellos que sean adecuados, pertinentes y no excesivos con los fines de investigación para los que se van a tratar.

c) Garantías para los derechos y libertades de los interesados. En particular, la anonimización y la seudonimización.

El art. 89.1 del RGPD establece que el tratamiento con fines de investigación científica estará sujeto a las garantías adecuadas, con arreglo al Reglamento, para los derechos y las libertades de los interesados, y ya conocemos que entre esas garantías resalta el secreto profesional. Pero, además, exige utilizar las técnicas de la anonimización y seudonimización. La LBAP y la LOPD no regulan la seudonimización. Sí lo hace la LIB.

El considerando 26 del RGPD gira en torno a la posibilidad o no de identificar a una persona física a través del tratamiento de sus datos personales, y diferencia datos

anónimos de datos seudonimizados señalando que: "*Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.*[31] *En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación."*

En suma, a los efectos del RGPD se considerará anonimización irreversible aquella en la que el esfuerzo exigido para la asociación de los datos personales y de salud no es razonable, resulta desproporcionado. Sin embargo, no conviene ignorar que esta conceptuación contiene un grado de indeterminación preocupante pues el uso y el descubrimiento de nuevas técnicas de asociación, posibilitará, sin duda, procesos exitosos de asociación de datos escindidos por compensar económicamente. De ahí que parece del todo razonable que se diseñen algunas garantías encaminadas a velar por que no se produzca la desanonimización, tales como la expresa prohibición legal de hacerlo y su tipificación como infracción administrativa muy grave.

[31] El grupo de trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales del artículo 29, creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, ha elaborado el Dictamen 05/2014 sobre técnicas de anonimización, de 10 de abril de 2014, tras describir las principales técnicas de anonimización, a saber, la aleatorización y la generalización, y abordar, en particular, el estudio de la adición de ruido, la permutación, la privacidad diferencial, la agregación, el anonimato k, la diversidad l y la proximidad t., y relatar los principios en que se basan estos métodos, sus fortalezas y debilidades, y los errores más comunes al aplicar las distintas técnicas, concluye el dictamen señalando que las técnicas de anonimización pueden aportar garantías de privacidad y usarse para generar procesos de anonimización eficientes, pero solo si su aplicación se diseña adecuadamente, lo que significa que han de definirse con claridad los requisitos previos (el contexto) y los objetivos del proceso para obtener la anonimización deseada al mismo tiempo que se generan datos útiles. La solución óptima debe decidirse caso por caso y puede conllevar la combinación de diversas técnicas, aunque siempre respetando las recomendaciones prácticas que se formulan en el dictamen. Señala también que los responsables del tratamiento deben ser conscientes de que un conjunto de datos anonimizado puede entrañar todavía riesgos residuales para los interesados, pues, por una parte, la anonimización y la reidentificación son campos de investigación activos en los que se publican con regularidad nuevos descubrimientos y, por otra, incluso los datos anonimizados, como las estadísticas, pueden usarse para enriquecer los perfiles existentes de personas, con la consiguiente creación de nuevos problemas de protección de datos. En suma, la anonimización no debe contemplarse como un procedimiento esporádico, y los responsables del tratamiento de datos han de evaluar regularmente los riesgos existentes.

El artículo 4 RGPD define la seudonimización como[32]:

> el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

El considerando 28 RGPD justifica la introducción de la seudonimización señalando que: "*La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.*" Lo que hace el RGPD es sustituir el consentimiento explícito de afectado por la técnica de la seudonimización.

La seudonimización es, por tanto, una medida útil de seguridad, pero que también permite un fácil acceso a la identidad del titular de los datos. Por ello, los datos seudonimizados deben estar protegidos por los principios y reglas del RGPD. Respecto de la anonimización, los expertos coinciden en que las técnicas actuales no garantizan al cien por cien que la anonimización sea irreversible. Mediante técnicas de ingeniería inversa se pueden conectar nuevamente los datos con sus titulares, aunque ello solo esté en manos de informáticos muy expertos. Hoy por hoy según los expertos esto parece irrefutable[33]. De ahí que el RGPD haga referencia al elemento de "razonabilidad" de los

---

[32] El citado dictamen 05/2014 conceptúa la anonimización y la seudonimización en los siguientes términos:
"*La anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación.*
La seudonimización consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo. La seudonimización no es un método de anonimización; simplemente, reduce la vinculabilidad de un conjunto de datos con la identidad original del interesado y es, en consecuencia, una medida de seguridad útil."
Ese grupo de trabajo también dijo que "*los datos cifrados son un ejemplo clásico de «seudonimización». La información contenida en esos datos se refiere a un individuo al que se asigna un código cifrado, mientras que la clave para descifrarlos, es decir para establecer la correspondencia entre el código y los identificadores habituales de la persona (nombre, fecha de nacimiento, dirección, etc.) se guardan por separado*". "*…los datos seudonimizados no constituyen información anonimizada, ya que permiten singularizar a los interesados y vincularlos entre conjuntos de datos diferentes. La probabilidad de que el seudoanonimato admita la identificabilidad es muy alta; por ello, entra dentro del ámbito de aplicación del régimen jurídico de la protección de datos. Esto reviste una especial relevancia en el contexto de las investigaciones científicas, estadísticas e históricas."*
Este dictamen analiza las diferentes técnicas de anonimización y seudonimización y los riesgos e inseguridades que conllevan.

[33] Al respecto, entre otros, MOGOLLÓN, S., "¿Existe de verdad la anonimización? El grupo del artículo 29 de Protección de Datos no lo pone fácil", en *Noticias Jurídicas,* Conocimiento, Artículos doctrinales, 20 de julio de 2014; Informe del experto núm. 12 *Acceso a la historia clínica con fines de investigación. Estado de la cuestión y controversias*, Fundación Salud 2000, julio de 2015, p. 12; GÓMEZ PIQUERAS, C., "Disociación/anonimización de los datos de salud" en *Revista Derecho y Salud,* vol. 18. Núm. 1, 2009, p. 56.

esfuerzos exigidos para identificar al titular de los datos una vez sometidos al proceso de anonimización, de manera que los considera anónimos si el esfuerzo exigido para la asociación no es razonable, entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados[34].

Para hacer operativas la anonimización o seudonimización en la investigación científica con utilización de historias clínicas, la entidad depositaria de los datos (Servicio autonómico de Salud o la Consejería) debe ceder los datos de salud anonimizados o seudonimizados, lo que exige disponer de un sistema que articule una opción de disociación automática[35] y el investigador, que los recibe disociados, los trata, solicitando y accediendo al código solo cuando imperiosamente necesita conocer a la persona, normalmente por razones epidemiológicas. Caso de no disponerse de la disociación automática, se ha planteado que la disociación la haga una persona distinta de aquellas que van a realizar la investigación[36].

d) Consentimiento de los interesados y papel de los Comités de Ética de Investigación.

En cuarto lugar, analizamos la peliaguda cuestión del consentimiento de los interesados. La enmienda introducida en el año 2014 por el Parlamento Europeo al proyecto de RGPD, supuso un serio hándicap para la investigación y estudios de salud, tanto clínicos como epidemiológicos y de salud pública, pues exigía el consentimiento explícito de los afectados para cada investigación o, en caso contrario, la anonimización irreversible. Empero, a la vista de la alarma que esta restricción suscitó en los investigadores y en las sociedades científicas, la Comisión Europea, el Parlamento Europeo y el Consejo, finalmente, llegaron a un acuerdo sobre el texto del reglamento en el que, conciliando del mejor modo posible la protección de datos de carácter personal con la investigación, se suprimen en buena parte las restricciones que había introducido el Parlamento Europeo, como comprobamos seguidamente.

De entrada, el artículo 5.1b) del RGPD establece que los datos personales

> serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»).

[34] En el mismo sentido, la Ley 14/2007 de Investigación Biomédica.

[35] El Grupo de trabajo sobre protección de datos del artículo 29 propuso el almacenamiento de los datos de salud en módulos, creando un módulo de investigación que dispusiera de un sistema que procediera a la disociación de la información en el momento de realizar su volcado en el módulo. Sobre esta temática, véase DE MIGUEL SÁNCHEZ, N., "Tratamiento de datos relativos a la salud: regulación en la normativa sanitaria y gestión a través de la historia clínica digital" en el libro colectivo *Derecho sanitario y bioética,* Tirant lo Blanch, 2011, pp. 278-281.

[36] DE MIGUEL SÁNCHEZ, N., "Tratamiento de datos relativos a la salud: regulación en la normativa sanitaria y gestión a través de la historia clínica digital" en el libro colectivo *Derecho sanitario y bioética,* Tirant lo Blanch, 2011, pp. 280.

Este artículo del RGPD significa que el uso de datos de salud en el ámbito de la investigación científica es compatible con el uso inicial para el que se recogieron los datos (asistencia sanitaria) por lo que no será necesario recabar un nuevo consentimiento de los sujetos cuyos datos se utilizan en la investigación. A esto hay que añadir el hecho de la ubicación de la investigación científica entre las circunstancias que enumera el artículo 9.2 RGPD, lo que obliga a entender que pueden tratarse datos con fines de investigación científica sin el consentimiento de los interesados, ello sin perjuicio de la adopción de medidas efectivas de disociación (anonimización, seudonimización) que garanticen el respeto del principio de minimización de los datos personales; de la adopción de normas dirigidas a respetar en lo esencial el derecho a la protección de datos; y del establecimiento de medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. Vemos, pues, que este apartado j) exige que el tratamiento lo sea sobre una base jurídica elaborada por el Derecho de la Unión o de los Estados miembros, que ha respetar en lo esencial el derecho a la protección de datos, y, a nuestro juicio, elemento esencial del derecho a la protección de datos es precisamente el consentimiento del interesado. Empero, concluir que en base a este requisito es plausible una norma que en todos los casos en que se haga investigación científica se exija el consentimiento de los interesados arrastraría la concurrencia de dos circunstancias -investigación científica y consentimiento-, cuando el inciso inicial del apartado 2 solo exige que concurra una circunstancia, que sería un fin de investigación científica.

No obstante, es plausible plantear la exclusión de los datos especialmente protegidos de la previsión del artículo 5.1.b) RGPD[37]. En efecto, respecto de los estudios observacionales no parece cabal excluir la necesidad de consentimiento de los interesados en la cesión de datos de salud contenidos en las historias clínicas y en otras fuentes para su ulterior tratamiento en cualquier investigación "científica" privada o pública, particularmente la privada en la que los beneficios no revierten en la ciudadanía[38]. Esta exclusión rompe con toda la legislación nacional e internacional y la

[37] Cuando la LOPD establece en su artículo 4.2 que "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquéllas para las que los datos hubieran sido recogidos", añade que "no se considerará incompatible el tratamiento posterior de éstos con fines históricos o científicos". No obstante, no puede obviarse que la actividad asistencial es una finalidad muy concreta, la asistencia sanitaria, y que el posterior uso de los datos obtenidos para investigación es un uso completamente diferente, y aunque el artículo 4 las considere actividades compatibles, debería ajustarse al principio de consentimiento previo sentado por la LOPD. Y, en efecto, el artículo 16.1 de la LBAP establece que "el acceso a la historia clínica con estos fines (de investigación o docencia) 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". Este artículo que excepciona la regla general del artículo 4.2 LOPD tiene su razón de ser, en mi criterio, en la consideración de los datos de salud como muy sensibles y especialmente protegidos.

[38] Se postula distinguir entre *legitimación legal*, que permite tratar datos con fines de atención sanitaria, calidad y gestión de servicios o fines de estudios epidemiológicos e investigación científica, y que se justifica en el interés público de esto fines, y *legitimación voluntaria*, que proviene siempre del consentimiento expreso del interesado y es la que se precia para tratar datos con fines estrictamente privados (desarrollo de las industrias sanitaria, farmacéutica y de biotecnología): *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública,* , Observatori de Bioética i Dret, Universitat de Barcelona, 2015, p. 40.

doctrina que hasta ahora viene exigiendo el consentimiento como regla general, y es muy poco respetuosa con el derecho fundamental a la protección de los datos personales. Cabe recordar que actualmente, sobre la base de nuestro Derecho, el tratamiento ulterior de datos de salud de historias clínicas cedidos con fines de investigación científica exige siempre el previo consentimiento del interesado salvo que los datos estén anonimizados. En las investigaciones con procedimientos invasivos tanto se hagan directamente con personas como con muestras biológicas almacenadas, es necesario consentimiento expreso para participar en la investigación, así como consentimiento para el tratamiento de los datos pues se le ha de informar sobre ello[39].

Supuesto lo anterior, seguidamente debemos preguntarnos si es lícito y ético obtener el consentimiento para hacer futuras investigaciones junto al inicial para la asistencia. La obtención del consentimiento informado para prestar la asistencia sanitaria lleva implícito el consentimiento tanto para elaborar la historia clínica como para su posterior archivo en un registro pues la LBAP no exige, como es lógico, un consentimiento específico para dichas actuaciones. Ello por cuanto ha de entenderse que la historia clínica es un elemento inherente e imprescindible de la asistencia sanitaria prestada. La LBAP dice que el fin principal de la historia clínica es facilitar la asistencia sanitaria, de donde se infiere que el legislador está contemplando otros posibles fines, que son, obviamente, utilizar las historias para evaluar la calidad del centro sanitario, así como para hacer estudios epidemiológicos e investigación sanitaria. Y no cabe duda de que las historias clínicas son una fuente muy importante, no la única, para hacer investigación científica sanitaria, por lo que, en nuestro criterio, no está demás que así se exprese en la norma que defina el alcance de estos documentos electrónicos. Aunque, como ya hemos razonado anteriormente en el apartado dedicado a la investigación sanitaria, la explicitación de este fin no ha de conllevar necesariamente que el consentimiento prestado para recibir la asistencia sanitaria sirva para la posterior utilización de la historia con fines de investigación. Es más, en razón de la debilidad psicológica en la que se encuentra la persona enferma que busca alivio a sus dolencias y la superioridad psicológica del profesional sanitario que le atiende en la relación clínica que se crea, en la mayoría de los casos podría considerarse no válido un consentimiento expreso, obtenido a la par que el consentimiento para recibir asistencia sanitaria, para un eventual uso posterior de los datos con fines de investigación sanitaria, por faltar o estar muy disminuidos los elementos de libertad, conocimiento y conciencia por parte del enfermo. Recuérdese que el considerando 32 del RGPD señala que "*El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. (...) El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar*

[39] Ambos consentimientos se recogen en el mismo documento.

innecesariamente el uso del servicio para el que se presta." Y que el considerando 43 añade "*Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento.*"

En apoyo de la posición que mantenemos sobre la necesidad de obtener un consentimiento expreso, parece oportuno transcribir la siguiente opinión del Observatorio de Bioética y Derecho. Ha dicho[40] que "*partiendo de la existencia del «partenariado público-privado» en el sistema sanitario e investigador, el problema se centra en cómo se articula la legitimación para usar la información de salud y reutilizarla. Es preciso tener en cuenta la gran asimetría -de información e incluso de poder- existente entre el ciudadano, que sufre una enfermedad y necesita curarse, y el profesional que le va a pedir el consentimiento, tanto para procurarle la asistencia médica más adecuada como para el tratamiento de los datos personales de salud. Hay que tener claro que se trata de consentimientos diferentes, y que el acceso a la prestación sanitaria pública no se puede condicionar al consentimiento para tratar datos con otros fines, ni justifica la solicitud de datos adicionales. La conclusión es que la obtención del consentimiento debe someterse a garantías, a fin de compensar la situación de desequilibrio en que se encuentra el usuario de los servicios sanitarios públicos en momentos en los que puede estar especialmente preocupado por su salud -lo que genera una situación de vulnerabilidad- y que piensa a priori que todos los datos que se le piden se encaminan a su tratamiento y son necesarios para prestarle la asistencia que necesita y que constituye la razón por la que ha acudido al sistema sanitario*." En fin, la situación de inferioridad psicológica, de vulnerabilidad, en la que se encuentra la persona que solicita asistencia sanitaria y otorga el consentimiento para recibirla, justifica que la utilización posterior de sus datos para otros fines se condicione a un nuevo consentimiento.

Otra cuestión no bien resuelta en el RGPD es si en necesario recabar un nuevo consentimiento cuando se quieren tratar datos obtenidos en una investigación para la que se obtuvo consentimiento para otra investigación posterior. Los considerandos 33 y siguientes del RGPD contemplan la circunstancia de que cuando no sea posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida, debe ofrecerse a los interesados

[40] Universidad de Barcelona. Observatorio de Bioética y Derecho, 2015, p. 42 Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para ello. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación, o partes de proyectos de investigación, en la medida que lo permita la finalidad perseguida. Conforme a este considerando es evidente que el RGPD no está por la labor de permitir un uso posterior absoluto de datos con fines científicos. Parece que deja a los Estados miembros la concreción de esta cuestión. Habrá, pues, que valorar en cada caso el alcance del consentimiento dado inicialmente. Para los casos en los que el consentimiento se dio para una concreta línea de investigación y las muestras se quieran utilizar posteriormente en otra línea de investigación distinta estimamos que debe obtenerse un nuevo consentimiento, habiéndose propuesto[41] que la solución pasa por un concepto dinámico de consentimiento, de manera que se diseñen mecanismos informáticos que permitan actualizarlo de una manera sencilla y ágil.

Finalmente, una referencia a la investigación científica privada con fin de lucro. Se afirma en el Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública[42], que resulta de especial importancia conseguir una protección gradual de los datos en función de la finalidad del uso, distinguiendo cuidadosamente las finalidades sanitaria, epidemiológica y de investigación y docencia, de las finalidades empresariales privadas basadas en la investigación a las que hay que exigir el nivel de protección más elevado. La legitimación voluntaria de un proyecto de investigación proviene siempre del consentimiento expreso del paciente y es la que se precisa para tratar datos con fines estrictamente privados, es decir, sin interés público evidente; este consentimiento es el que se requiere para utilizar los datos de los usuarios en el desarrollo de las industrias sanitarias, farmacéuticas y de biotecnología, o la promoción y comercialización de sus productos.

Así las cosas, parece conveniente que el legislador, haciendo uso de la habilitación del artículo 9.4 RGPD, introduzca condiciones adicionales o limitaciones al tratamiento de datos en investigaciones científicas, particularmente en las realizadas por entidades privadas con fin de lucro de manera que la investigación científica que realicen los sea siempre con datos anonimizados irreversiblemente o con previo consentimiento escrito de los interesados. Y en los casos en los que sea necesaria la exención del consentimiento informado, debe ser imprescindible un dictamen favorable del Comité de Ética de Investigación.

6. Utilización de tecnologías que permitan tratar a gran escala datos provenientes de fuentes dispares.

[41] Federico DE MONTALVO "La genética está revolucionando conceptos clásicos como el CI" en Diario Médico de 23 de mayo de 2016, Disponible en http://www.diariomedico.com/especial/xxiv-aniversario-dm/la-genetica-esta-revolucionando-conceptos-clasicos-como-el-ci.

[42] Publicado por el Observatorio de Bioética y Derecho, Universidad de Barcelona, 2015. Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

Propuesta de regulación:

Opción A:

1. El tratamiento de datos de salud a gran escala obtenidos directamente de Internet, como foros de debate, redes sociales y otros sitios online, mediante tecnologías que permiten tratar cantidades masivas de datos provenientes de fuentes dispares, exigirá el consentimiento del sujeto para su tratamiento en investigación sanitaria o epidemiología social salvo que el sujeto los haya hecho manifiestamente públicos[43] *y así lo acredite el investigador o el responsable del tratamiento.*

Opción B.

1. El tratamiento de datos de salud a gran escala mediante tecnologías que permiten tratar cantidades masivas de datos provenientes de fuentes dispares, siempre exigirá una previa evaluación de un comité de ética de la investigación que deberá realizar las funciones asignadas por el artículo 12.2 de la Ley 14/2007, de 3 de julio, de Investigación Biomédica.

2. Los datos obtenidos deberán ser adecuados a la finalidad que motiva su recogida.

3. Se establecerán las siguientes medidas de seguridad en el tratamiento masivo de datos de salud[44]*:*

a) anonimización de los datos.
b) cuando no sea posible o conveniente la anonimización de los datos, seudonimización de los datos mediante método de encriptación, tanto en el lugar de almacenamiento como durante las transferencias de datos.
c) las medidas de autenticación de los sujetos que accedan a los datos deben ser del más alto nivel.
d) Los datos se destruirán una vez finalizado el tratamiento programado.

4. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales

[43] Una reciente sentencia del Tribunal Supremo, de 15 de febrero de 2017 -RJ/2017/36954-, afirma que la finalidad de una cuenta abierta en una red social en Internet es la comunicación de su titular con terceros y la posibilidad de que esos terceros puedan tener acceso al contenido de esa cuenta e interactuar con su titular, pero no que pueda publicarse la imagen del titular de la cuenta en un medio de comunicación. Ello, obviamente, porque no es su intención hacer su imagen manifiestamente pública.

[44] Tomado del trabajo de GIL. E., *Big data, privacidad y protección de datos, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS- AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO, 2016, p. 142.* Escribe la autora que "Tal y como señala Ira S. Rubinstein, este sistema está alineado con los principios de protección de datos europeos, al tiempo que ofrece una solución a los problemas que el big data impone sobre la gestión de los datos y la privacidad de los individuos."

medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas[45].

5. El responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

6. En aquellos casos de uso de datos masivos en que las dimensiones del análisis hacen inviable la obtención del consentimiento informado de todos los sujetos implicados, una vez evaluado el impacto de las operaciones de tratamiento en la protección de datos de carácter personal, la autoridad de control deberá aprobar la evaluación del impacto y la ejecución del estudio.

7. Cuando un responsable esté autorizado a efectuar un análisis con datos masivos, deberá ofrecer a los sujetos participantes la posibilidad de rechazar su participación mediante la opción de exclusión voluntaria (cláusula de no participación). Con ese fin, se pondrán en marcha los sistemas de información pública necesarios para permitir ejercer esa opción de exclusión voluntaria o para ejercitar los derechos establecidos en los artículos 15 a22 del Reglamento (UE) 2016/679, de 27 de abril de 2016.

8. Queda prohibido tomar decisiones de tratamientos individuales automatizados, incluida la elaboración de perfiles, que se base únicamente en datos relativos a la salud, datos genéticos, datos biométricos y datos relativos a la vida sexual y orientación sexual, salvo que el interesado haya dado su consentimiento explícito[46].

Comentario exegético:

a) Riesgos del *big-data* y consentimiento del interesado.

El RGPD no determina qué debe entenderse por "gran escala". El Grupo del artículo 29, considera que para valorar si el tratamiento se realiza a gran escala debe tenerse en cuenta:
a) El número de interesados afectados, bien en términos absolutos, bien como proporción de una determinada población
b) El volumen de datos y la variedad de datos tratados
c) La duración o permanencia de la actividad de tratamiento
d) La extensión geográfica de la actividad de tratamiento

CASACUBERTA[47] nos ha mostrado cómo la epidemiología ha avanzado gracias al fenómeno del *big data* (masivas bases de datos alimentadas en tiempo real con millones de entradas que pueden procesarse para buscar correlaciones de forma rápida) y de qué

[45] Artículo 25.2 del RGPD
[46] Artículo 22.4 del RGPD.
[47] "Innovación, Big Data y Epidemiología" en *Revista Iberoamericana de Argumentación*, núm. 7, 2013, pp. 1-12.

manera este fenómeno puede ser una poderosa herramienta para seguir innovando en epidemiología, al permitir trabajar con grandes poblaciones en tiempo real, y aumentar así las posibilidades de establecer correlaciones estadísticas lo suficientemente argumentadas para poder inferir la realidad del fenómeno y buscar posibles mecanismos causales con al menos cierta probabilidad de llegar a un resultado fiable

El Grupo del artículo 29 pone como ejemplo de tratamiento a gran escala el tratamiento de datos de pacientes en el desarrollo normal de la actividad de un solo hospital. El considerando 91 del RGPD señala específicamente que no debe considerarse que el tratamiento de datos personales se realiza a gran escala si el tratamiento concierne a datos personales de pacientes a cargo de un médico u otro profesional sanitario, por lo que en estos casos la evaluación de impacto de la protección de datos no debe ser obligatoria. No cabe duda, pues, que el tratamiento masivo de datos obtenidos de registros de centros sanitarios constituye un tratamiento a gran escala.

Además, con la generalización de la historia clínica electrónica y la receta electrónica más los datos obtenidos directamente de Internet podemos disponer actualmente de ficheros y archivos electrónicos con cantidades ingentes de datos de salud, lo que permite un tratamiento automatizado a gran escala de esos datos (*big-data*), algo que indudablemente es óptimo para la investigación científica, si bien también incrementa notablemente el riesgo de violar la intimidad de los sujetos titulares de los datos dado que: a) se obtienen y se tratan sus datos sin que su titular lo conozca, b) el deber de secreto por sí solo resulta poco operativo como medida de seguridad ya que personas expertas en informática pueden acceder con relativa facilidad a dichos archivos electrónicos e interceptar transmisiones de datos informáticos, por lo que en el año 2015 se ha incorporado al Código Penal como delito (art. 197 bis), c) la anonimización ha dejado de ser irreversible pues ya se disponen de técnicas para la reidentificación[48].

[48] En el citado "Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública" se hace la siguiente advertencia: "Como se ha dicho, en estos momentos, las evidencias técnicas ya nos muestran que es posible re-identificar a personas concretas a partir de los datos de un dataset sobre el cual se han aplicado técnicas de anonimización (o desidentificación). Una persona, o una empresa, puede conseguir la re-identificación si tiene la voluntad (por razones económicas, empresariales, delictivas...), los conocimientos y los medios técnicos para ello (por ejemplo, con los datos sanitarios de un hospital -sin datos personales- y acceso a los datos personales de otro dataset -digamos, un censo-). Parece evidente que, en el caso de los datos de salud, es fácil encontrar ese hipotético «adversario» con la motivación y los recursos para poder hacerlo y, por lo tanto, es acertado cuestionar la validez de las iniciativas de intercambio de datos sensibles que estén basadas en técnicas de anonimización. En el ámbito jurídico, el incierto recurso a la «anonimización», entendida como una solución definitiva pero irremediablemente en crisis, viene propiciado por la actual normativa de protección de datos cuyo origen se halla en una Directiva europea del año 1995, muy anterior al fenómeno del Big Data, y subyace en la Ley estatal 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. Sin embargo, desde el momento en que el propio anonimato deviene incierto es perentorio encontrar una base que legitime el análisis de datos personales de salud a gran escala. De no ser así, se abre la puerta a usos no deseados de esos datos ya que su titular, habiendo dado su consentimiento para determinadas acciones en el ámbito sanitario y de investigación, en realidad pierde el control y queda desprotegido pues -con una falsa concepción de la protección de datos y del secreto profesional- desconoce que sus datos pueden haber sido utilizados o cedidos para otros fines, ni deseados ni efectivamente consentidos."

ALTISENT TROTA[49], ha señalado que la potencialidad de las nuevas tecnologías genera un temor que está llevando a multiplicar las normas jurídicas para proteger la intimidad[50]. En la línea de potenciar instrumentos dirigidos a garantizar la intimidad cabe recordar que el RGPD ha introducido el denominado «derecho al olvido» que faculta a los ciudadanos europeos a pedir el borrado de sus datos bajo determinados requisitos y con las excepciones que comentaremos más adelante.

El problema radica en conciliar el procesamiento y tratamiento a gran escala de datos de salud y la intimidad de los titulares de esos datos. Al respecto, en nuestra opinión caben dos opciones.

Opción A. Exigir el previo consentimiento de los titulares de los datos. Los datos masivos proceden de diferentes fuentes de información: redes sociales, laborales, ambientales, de salud, de negocios, del ocio, etc. y la investigación en Internet plantea serios problemas respecto a la privacidad de los datos personales que se pueden obtener. Actualmente, existen muchos foros *online* en los que se exponen datos sensibles (salud sexual, reproducción asistida, abortos, diagnósticos médicos, etc.). Aunque la información esté disponible *online* es lógico pensar que las personas no esperan ni desean que esa información sea recogida por terceros extraños a su círculo para ser usada con fines de investigación. En algunos casos podrían dar su consentimiento y en otros muchos probablemente negarían ese uso.[51]

Señala Elena GIL[52] que el RGPD, incluso en el *big data*, continúa confiando en el consentimiento informado como primera herramienta para proteger los datos y la privacidad de los ciudadanos europeos; de hecho, se refuerza la importancia del consentimiento.

Una reciente sentencia del Tribunal Supremo, de 15 de febrero de 2017 -JUR/2017/36954- afirma que la finalidad de una cuenta abierta en una red social en Internet es la comunicación de su titular con terceros y la posibilidad de que esos terceros puedan tener acceso al contenido de esa cuenta e interactuar con su titular, pero no que pueda publicarse la imagen del titular de la cuenta en un medio de comunicación. Ello, obviamente, porque no es su intención hacer su imagen manifiestamente pública. Concretamente razona el TS que "*Tener una cuenta o perfil en una red social en Internet, en la que cualquier persona puede acceder a la fotografía del titular de esa cuenta, supone que el acceso a esa fotografía por parte de terceros es lícito, pues está autorizada por el titular de la imagen. Supone incluso que el titular de*

[49] ALTISEN TROTA, R, voz "Confidencialidad" en ROMEO CASABONA (director) *Enciclopedia de Bioderecho y Bioética,* Comares S.L., 2011, Tomo I, p. 429.

[50] Por ejemplo, la Ley Orgánica 1/2015, de 30 de marzo, ha modificado el Código Penal introduciendo el artículo 197bis por el que se castiga como actividad delictiva la piratería informática tanto en el acceso a archivos como en la interceptación de transmisiones de datos.

[51] En este sentido, SANTI, M.ª F., "Controversias éticas en torno a la privacidad, la confidencialidad y el anonimato en investigación social", en *Revista de Bioética y Derecho*, 2016, núm. 37, pp. 17-18.

[52] Gil, E. *Big data, privacidad y protección de datos*, Agencia Española de Protección de Datos, 2016, p.54.

la cuenta no puede formular reclamación contra la empresa que presta los servicios de la plataforma electrónica donde opera la red social porque un tercero haya accedido a esa fotografía cuyo acceso, valga la redundancia, era público. Pero no supone que quede excluida del ámbito protegido por el derecho a la propia imagen la facultad de impedir la publicación de su imagen por parte de terceros, que siguen necesitando del consentimiento expreso del titular para poder publicar su imagen."

Empero, también escribe Elena GIL[53] que "Numerosos autores opinan que los deberes de información y la necesidad de recabar el consentimiento debe referirse, no solo al hecho de que se recaben datos primarios, sino también a la información que se puede extraer de un análisis sofisticado de estos, incluyendo la información que pueda extraerse de la agregación de datos que recaba la empresa con datos provenientes de otras fuentes y ficheros. No obstante, esta aproximación tiene muchas dificultades prácticas, en tanto que, por su propia naturaleza, el valor del *big data* reside precisamente en lo inesperado de los resultados que revela. Así, ¿cómo explica el responsable del tratamiento que resulta imposible saber con antelación qué información revelará el tratamiento de los datos recabados? Son muchos los autores que consideran que el consentimiento prestado bajo estas circunstancias no es el consentimiento informado que la ley exige."

Además, en la práctica es viable obtener el previo consentimiento de un sujeto para utilizar su imagen o sus datos por terceros en una investigación científica, pero es inviable, pues implica un esfuerzo desproporcionado, obtener ese consentimiento de miles, incluso millones, de sujetos que han depositado datos personales en cuentas abiertas en redes sociales. Conseguir esos consentimientos haría inviable cualquier proyecto de investigación científica. De ahí que, en nuestro criterio, parece más razonable la opción B.

Opción B. Sustituir el consentimiento de los interesados por una evaluación y control de un Comité de Ética de Investigación que vele por la protección de los derechos de los titulares de los datos y dé garantía pública de los proyectos de investigación, evaluando su corrección metodológica, ética y legal.

La investigación científica debe realizarse en condiciones de respeto a los derechos fundamentales de la persona y a los postulados éticos que afectan a la investigación biomédica en la que resultan afectados seres humanos, siguiéndose, a estos efectos, la Declaración de Helsinki y cualesquiera otros instrumentos internacionales suscritos por España en esta materia.

Para evaluar los proyectos de investigación y velar por el respeto de los derechos humanos, la LIB, en su artículo 12, regula los Comités de Ética de Investigación, de composición interdisciplinar, a los que asigna las siguientes funciones:

[53] Cit. p. 73.

a) Evaluar la cualificación del investigador principal y la del equipo investigador así como la factibilidad del proyecto.
b) Ponderar los aspectos metodológicos, éticos y legales del proyecto de investigación.
c) Ponderar el balance de riesgos y beneficios anticipados dimanantes del estudio.
d) Velar por el cumplimiento de procedimientos que permitan asegurar la trazabilidad de las muestras de origen humano, sin perjuicio de lo dispuesto en la legislación de protección de datos de carácter personal.
e) Informar, previa evaluación del proyecto de investigación, toda investigación biomédica que implique intervenciones en seres humanos o utilización de muestras biológicas de origen humano, sin perjuicio de otros informes que deban ser emitidos. No podrá autorizarse o desarrollarse el proyecto de investigación sin el previo y preceptivo informe favorable del Comité de Ética de la Investigación.
f) Desarrollar códigos de buenas prácticas de acuerdo con los principios establecidos por el Comité Español de Ética de la Investigación y gestionar los conflictos y expedientes que su incumplimiento genere.
g) Coordinar su actividad con la de comités similares de otras instituciones.
h) Velar por la confidencialidad y ejercer cuantas otras funciones les pudiera asignar la normativa de desarrollo de esta Ley.

No cabe duda de la importancia de estos órganos técnicos, independientes e imparciales, para evaluar y, en su caso, informar preceptivamente proyectos de investigación en los que no pueda obtenerse el consentimiento de las personas afectadas o se utilicen datos de salud masivos (big-data).

b) Elaboración de perfiles[54].

El artículo 4.4 del RGPD define «elaboración de perfiles» como

> Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales,

[54] Un perfil de género y salud es un resumen de datos e información relacionada que describe la salud y sus factores determinantes para una población dada. El contenido de un perfil se basa en datos tanto numéricos (cuantitativos) como narrativos (cualitativos). Los datos numéricos dan una idea de lo que está sucediendo (por ejemplo, tendencias con el transcurso del tiempo, aparición de nuevas enfermedades o problemas de salud) y a quién está sucediendo (por ejemplo, qué personas están enfermas, dónde viven, qué tratamiento están recibiendo). Los datos numéricos describen la salud de la población en forma general, mientras que el análisis y la investigación estadística permiten comparar las variables desglosadas por sexo y edad, con otras variables complementarias. Sin embargo, los datos numéricos no son la única información suministrada en un perfil; la investigación académica actual, los documentos oficiales y los informes de la comunidad suministran otra información valiosa para un perfil acerca de por qué se observan las tendencias y cómo se llegó a ellos. Por lo tanto, un perfil de género y salud debe incluir una amplia gama de indicadores para la salud y los factores determinantes de la salud. Es decir, un perfil deberá incluir no solo indicadores clínicos de salud física y mental, sino también indicadores acerca de otras dimensiones de la vida de las personas. (Copiado del documento "Elementos para Elaborar un Perfil de Género y Salud", ", disponible en: http://new.paho.org/hq/dmdocuments/2009/Perfil-ESP.pdf).

intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Por su parte, el artículo 22, rubricado "Decisiones individuales automatizadas, incluida la elaboración de perfiles" establece en lo que aquí interesa los siguiente:

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:
a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a)[55] o g)[56], y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Los considerando 71 y 75 del RGPD recuerdan que los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización, así como en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos a la salud con el fin de crear o utilizar perfiles personales. De ahí que el interesado tenga derecho a no ser objeto de una decisión que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, y que este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con la salud.

[55] a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

[56] g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. Este apartado se refiere a los otros supuestos de punto 1 del artículo 9. Afectan a la soberanía del Estado, prevención del terrorismo, de la delincuencia organizada, etc.

En lo que hace a los datos de salud, se afirma en el "Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública"[57] lo siguiente: "*Partiendo del reconocimiento del principio de autonomía de las personas, la implementación de las tecnologías Big Data en salud, asociada a una eventual comercialización de dichos datos, produce un impacto en nuestro sistema sanitario e investigador y afecta directamente a la esfera privada de los ciudadanos. (...). Los riesgos potenciales no son hipotéticos, ni remotos: es suficiente con analizar la posibilidad de construir perfiles de conducta sobre datos anónimos, que se pueden utilizar en cualquier momento para tomar decisiones automatizadas sobre las personas. Basta un paseo por internet para encontrar una buena cantidad de empresas dedicadas a la compraventa de datos y constatar que las que los poseen -originados en la prestación de otros servicios- crean a su vez otras nuevas empresas y líneas de negocio dedicadas a la reutilización de estos datos consiguiendo perfiles muy precisos mediante sucesivos cruces de información y demás procesos de «enriquecimiento del dato*".

Se trata, pues, de prohibir la elaboración de perfiles personales con datos de salud para predecir aspectos relativos, entre otros, a la salud de las personas salvo que el interesado haya dado su consentimiento explícito. Sin el consentimiento del interesado solo pueden elaborarse perfiles por razones de interés público esencial, concepto este en el que solo se comprenden temas como la soberanía del Estado, prevención del terrorismo y de la delincuencia organizada, etc.

c) Evaluación de impacto.

El RGPD supone un avance en la protección de los datos de salud al definirlos de forma amplia, lo que evita que escapen de su ámbito los datos obtenidos con las nuevas tecnologías cuyo análisis conjunto con otros datos puede revelar información sobre el estado de salud de las personas. A tenor de la definición de tratamiento de datos personales contenida en el RGPD el *big-data* constituye un tratamiento de datos personales[58]. Empero, no encontramos en el RGPD ni en el proyecto de la nueva LOPD una regulación específica para el *big-data* que dé particular respuesta a los problemas de seguridad y privacidad[59]. El RGPD ha introducido la obligación por los responsables del tratamiento de realizar evaluaciones de impacto sobre la privacidad en todos los procesos en los que haya tratamiento masivo de datos personales, pero no incorpora una

[57] Observatorio de Bioética y Derecho, Universidad de Barcelona, 2015, pp. 40-42 Disponible en: http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf

[58] SERRANO PÉREZ, Mª. M., ibidem, p. 52.

[59] En el Informe de Experto, núm. 12, de la Fundación 2000, julio-2015, titulado "Acceso a la historia clínica con fines de investigación. Estado de la cuestión y controversias", en el apartado dedicado al *big-data* se dice: "A lo anterior hay que añadir que la reutilización masiva de datos sanitarios no parece un sistema previsto por la legislación vigente (no se trata de un proceso de investigación al uso como hasta ahora viene funcionando, esto es, bajo las coordenadas de la Ley de autonomía del paciente y de la legislación de protección de datos), sino uno nuevo con mucha trascendencia al exterior, cesión a terceros, subcontratación y configuración como un posible producto comercializado. En tal sentido, el establecimiento de esta nueva categoría de tanta trascendencia debería ser objeto, previamente, del debate público correspondiente, de una decisión de mayor consenso y prudencia y con toda probabilidad de un mayor rango legal."

regulación específica. La evaluación de impacto ha de realizarse, entre otros supuestos, en el tratamiento a gran escala de las categorías especiales de datos de salud, biomédicos y genéticos pues establece el artículo 35 RGPD que:

> 1.Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.
>
> 2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.
>
> 3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
> (…)
> b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1.

Además, el artículo 36.1 del RGPD establece que:

> El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo

La Guía para una Evaluación de Impacto en la Protección de Datos personales (EIPD) elaborada por la Agencia Española de Protección de Datos[60] nos dice que un EIPD es, en esencia, un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados y, tras ese análisis, poder afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos, y que la gran ventaja derivada de la realización de una EIPD en las etapas iniciales del diseño de un nuevo producto, servicio o sistema de información es que permite identificar los posibles riesgos y corregirlos anticipadamente, evitando los costes derivados de descubrirlos a posteriori, cuando el servicio está en funcionamiento o, lo que es peor, cuando la lesión de los derechos se ha producido. Añade que, además, la realización de una EIPD es un excelente ejercicio de transparencia, base de una relación de confianza. El artículo 30.2.f) del anteproyecto de nueva LOPD también prevé la realización de una evaluación de impacto.

7. Investigación con muestras biológicas y consentimiento del interesado.

Propuesta de regulación:

[60] Agencia Española de Protección de Datos, Guía para una Evaluación de Impacto en la Protección de Datos personales, disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

1. El consentimiento para participar en una investigación biomédica y el consentimiento para el tratamiento de los datos deben ser específicos, si bien pueden plasmarse en el mismo documento.

2. El consentimiento del sujeto fuente será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización.

No obstante lo anterior, de forma excepcional podrán tratarse muestras pseudonimizadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable. En estos casos se exigirá el dictamen favorable del Comité de Ética de la Investigación correspondiente, el cual deberá tener en cuenta, como mínimo, los siguientes requisitos:

a) Que se trate de una investigación de indudable valor social.
b) Que el estudio no plantee más que un riesgo mínimo para los sujetos participantes.
c) Que la investigación sea menos efectiva o no sea posible sin los datos identificativos del sujeto fuente.
d) Que no conste una objeción expresa del mismo.
e) Que se garantice la confidencialidad de los datos de carácter personal.

3. Las muestras biológicas obtenidas ante de la entrada en vigor de la Ley 14/2007, de 3 de julio, de Investigación Biomédica, podrán ser tratadas con fines de investigación biomédica cuando el sujeto fuente haya dado su consentimiento o cuando las muestras hayan sido previamente anonimizadas.

Comentario exegético:

El RGPD concibe la muestra biológica[61] como un soporte de datos personales relativos a la salud por lo que su tratamiento debe acomodarse a todas las reglas establecidas para el tratamiento de datos de salud. Como ha apuntado NICOLÁS JIMÉNEZ[62] la posibilidad de anonimizar las muestras biológicas a efectos de excluir su tratamiento del RGPD y demás reglas sobre protección de datos se ha cuestionado toda vez que el genoma humano es propio de un solo individuo. De ahí que la LIB haya optado por exigir el consentimiento del sujeto fuente se proceda o no a la anonimización.

Conforme a los artículos 4 y 5 LIB el consentimiento para participar en una investigación y el consentimiento para el tratamiento de los datos deben ser específicos, si bien pueden plasmarse en el mismo documento. La cesión de muestras, aunque estén

[61] Según el artículo 3 de la LIB muestra biológica es cualquier material biológico de origen humano susceptible de conservación y que pueda albergar información sobre la dotación genética característica de una persona.
[62] NICOLÁS JIMÉNEZ, P, voz "Muestra biológica", en ROMEO CASABONA (director) *Enciclopedia de Bioderecho y Bioética,* Tomo II, Editorial Comares, S.L., 2011, p. 1139.

codificadas, también requiere consentimiento. El art. 58 LIB establece el régimen general y en el último párrafo un régimen especial:

> 1. La obtención de muestras biológicas con fines de investigación biomédica podrá realizarse únicamente cuando se haya obtenido previamente el consentimiento escrito del sujeto fuente y previa información de las consecuencias y los riesgos que pueda suponer tal obtención para su salud. Dicho consentimiento será revocable.
> 2. El consentimiento del sujeto fuente será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización.
> No obstante lo anterior, de forma excepcional podrán tratarse muestras codificadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable en el sentido del artículo 3.i) de esta Ley. En estos casos se exigirá el dictamen favorable del Comité de Ética de la Investigación

Sobre el consentimiento se explica en el preámbulo de la LIB que todo el marco jurídico establecido gira en torno al consentimiento del sujeto fuente de la muestra biológica y a la información previa que a este respecto debe serle suministrada. En cuanto a la disyuntiva sobre la posibilidad de que el sujeto fuente otorgue un consentimiento completamente genérico o uno específico sobre el uso o posteriores usos de la muestra, la LIB opta por un régimen intermedio y flexible, en el sentido de que el consentimiento inicial puede cubrir, si así se ha previsto en la información proporcionada previamente al sujeto fuente, investigaciones posteriores relacionadas con la inicial, incluidas las investigaciones que puedan ser realizadas por terceros y las cesiones a estos de datos o muestras identificados o identificables. En todo caso, como apunta BOMBILLAR SÁENZ[63], lo que no es del todo correcto es una suerte de consentimiento presunto, de presunción legal por la que las muestras biológicas obtenidas con fines diagnósticos y terapéuticos puedan utilizarse con fines de investigación biomédica. En suma, acertadamente afirma BOMBILLAR SÁENZ que "no caben documentos de consentimiento informado totalmente descontextualizados del estudio (o estudios) a los que dicen servir. No cabe amparar bajo consentimientos informados estándar la toma de muestras para una genérica utilización de datos clínicos y material biológico para realizar futuros estudios de investigación biomédica. No es posible escudarse en términos laxos e indeterminados para configurar una suerte de cheque en blanco en el que cualquier investigación basada en estas muestras pueda tener cabida."

El referido régimen flexible exige, por tanto, que en la información sobre la finalidad de la investigación se informe sobre la posibilidad de la realización de posteriores investigaciones relacionadas con la inicial, incluyendo, en su caso, que estas pueden ser realizadas por terceros, así como sobre las cesiones de datos o muestras identificadas o identificables. Cuando lo consentido por el sujeto fuente sea únicamente la utilización para una investigación determinada la falta de esta información complementaria conllevará la necesidad de recabar un nuevo consentimiento informado. Así, la descripción del proyecto de investigación o, en su caso, las investigaciones o líneas de

63 "Tratamiento jurídico del consentimiento informado y la donación de muestras biológicas a un biobanco para investigación biomédica: los consentimientos en blanco", en *Derecho y Salud,* vol. 27, núm. 1, 2017, p. 121 y ss.

investigación para las que se va a utilizar la muestra deben aparecer entre la información al sujeto fuente, además de la constancia expresa de que la muestra solo pueda ser utilizada en el ámbito de las finalidades indicadas El sujeto fuente, en garantía de su derecho a disponer sobre sus muestras, puede introducir restricciones sobre el uso de las mismas.[64]

Excepcionalmente, la LIB prevé la utilización de muestras obtenidas con una finalidad distinta que puedan identificar al sujeto fuente sin su consentimiento en los casos en que la obtención del consentimiento no sea posible o represente un esfuerzo no razonable[65]. El artículo 24 del Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica, establece que "se entenderá esfuerzo no razonable el que suponga el empleo de una cantidad de tiempo, gastos y trabajo desproporcionado."

El segundo pilar de esta regulación es la necesidad de obtener un dictamen favorable del Comité de Ética de Investigación, ello, como apunta NICOLÁS JIMÉNEZ[66] a pesar de que los riesgos físicos de la investigación con muestras biológicas son inexistentes, puesto que se trata de una investigación *in vitro* (aparte del procedimiento invasivo para su obtención).

Finalmente, señalar que la disposición transitoria segunda de la LIB contempla el importante número de muestras biológicas obtenidas ante de su entrada en vigor, disponiendo que podrán ser tratadas con fines de investigación biomédica cuando el sujeto fuente haya dado su consentimiento o cuando las muestras hayan sido previamente anonimizadas.

8. Difusión o publicación de los resultados de la investigación[67].

Propuesta de regulación.

Al objeto de garantizar la confidencialidad de la información clínica, a efectos de su difusión o publicación se tendrán en cuenta necesariamente las siguientes normas:

a) No se difundirán aquellos datos que permitan la identificación de los sujetos participantes.

---

[64] Véase en este sentido, GIL, C., "Utilización de muestras biológicas de origen humano con fines de investigación", en Revista de Bioética y Derecho, núm. 25, 2012, versión On-line. Disponible en: <http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886588720120002000003&lng=es&nrm=iso>

[65] Régimen excepcional traído del artículo 22 de la Recomendación (2006) 4 del Consejo de Europa.

[66] "Donación y utilización de material biológico humano con fines de investigación biomédica", en (A. PALOMAR OLMEDA y J. CANTERO RODRÍGUEZ, dirección) *Tratado de Derecho Sanitario,* vol. II, ARANZADI, 2013, pp. 963-964.

[67] Seguimos el artículo 11 del Decreto 29/2009, de 5 de febrero, de Galicia, de uso y acceso a la historia clínica electrónica.

b) Cuando sea absolutamente necesario identificar a los sujetos participantes, será preceptiva la autorización por escrito de los mismos.

c) Cuando sea necesaria la publicación de imágenes médicas o cualquier otro soporte audiovisual que muestren partes del cuerpo de los sujetos participantes y de ellas se pudiera llegar a conocer su identidad, será obligatoria la autorización escrita de los mismos.

d) La difusión o publicación de resultados seguirá en todo caso las normas y sugerencias relativas a la buena práctica en investigación.

Comentario exegético:

La etapa final de una investigación científica es hacer públicos los resultados de esa investigación para que sean conocidos por la comunidad científica y las autoridades pertinentes. La divulgación de la investigación científica, mediante artículos, ponencias y conferencias, entre otros mecanismos, es esencial, pues, como comúnmente se reconoce, investigación que no se publica no existe. Se puede decir que la investigación culmina con su publicación en una revista científica y su depósito en versión electrónica en repositorios de acceso abierto[68]; solo así será conocida por la comunidad científica, sus resultados serán discutidos y contribuirá al conocimiento científico universal.

Esa publicación, obviamente, ha de preservar la intimidad de los sujetos participantes en la investigación. Señala al respecto el considerando 159 del RGPD que "*Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas*."

Más concretamente, el artículo 27.3 de la LIB establece:

> Los investigadores deberán hacer públicos los resultados generales de las investigaciones una vez concluidas, atendiendo a los requisitos relativos a los datos de carácter personal a los que se refiere el artículo 5.5 de esta Ley y sin menoscabo de los correspondientes derechos de propiedad intelectual e industrial que se pudieran derivar de la investigación.

El citado artículo 5.5 establece:

> Si no fuera posible publicar los resultados de una investigación sin identificar a la persona que participó en la misma o que aportó muestras biológicas, tales resultados sólo podrán ser publicados cuando haya mediado el consentimiento previo y expreso de aquélla.

[68] Véase el artículo 37 de la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

9. Límites a los derechos de los interesados en el ámbito de la investigación científica.

Propuesta de regulación:

1. No será aplicable la obligación del responsable del tratamiento de comunicar la información enumerada en el punto 1 del artículo 15 del Reglamento (UE) 2016/679, de 27 de abril de 2016, en los siguientes casos[69]*:*

a) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado para el tratamiento con fines de investigación científica, o en la medida en que la obligación de información pueda imposibilitar u obstaculizar gravemente el logro de los fines científicos perseguidos por la investigación. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información.

b) la obtención o la comunicación de los datos esté expresamente establecida por la legislación que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado.

c) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada, incluida una obligación de secreto de naturaleza estatutaria

2. No será aplicable el derecho de rectificación establecido en el artículo 16 del Reglamento (UE) 2016/679, de 27 de abril de 2016, cuando el ejercicio de dicho derecho pueda imposibilitar u obstaculizar gravemente el logro de los fines científicos perseguidos por la investigación y se haya procedido a la seudonimización de los datos.

3. No será aplicable el derecho a obtener del responsable del tratamiento la limitación del tratamiento en las condiciones enumeradas en los apartados a)[70] *y d)*[71] *del punto 1 del artículo 18 del Reglamento (UE) 2016/679, de 27 de abril de 2016, cuando el ejercicio de dicho derecho pueda imposibilitar u obstaculizar gravemente el logro de los fines científicos perseguidos por la investigación.*

4. El interesado no podrá ejercer el derecho de oposición al tratamiento de sus datos personales establecido en el artículo 21 del Reglamento (UE) 2016/679, de 27 de abril de 2016, cuando el tratamiento sea necesario para la realización de estudios epidemiológicos e investigaciones sanitarias de interés público en el ámbito de la salud pública. No obstante, el responsable deberá acreditar los intereses públicos que prevalecen sobre los derechos de los interesados.

---

[69] Supuestos enumerados en el artículo 14.5 del RGPD.

[70] a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

[71] d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

5. El interesado o los familiares del interesado fallecido no pueden exigir la supresión de sus datos de salud cuando pueda causarle un perjuicio o a un tercero o cuando no haya transcurrido el plazo mínimo fijado por la legislación sanitaria. Transcurrido ese plazo, los datos no se destruirán, sino que se bloquearán, conservándose únicamente a disposición de los Administraciones públicas y Jueces y Tribunales para la atención de posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de estas, así como por razones epidemiológicas y de investigación sanitaria.

Comentario exegético:

El RGPD contempla la posibilidad de limitar algunos de los derechos de los interesados relacionados con el tratamiento de sus datos. Así, el artículo 89.2 establece que cuando el tratamiento de los datos personales se realice con fines de investigación científica la legislación de la Unión o de un Estado miembro podrá establecer excepciones a los derechos regulados en los artículos 15 (derecho de acceso del interesado a los datos y a obtener información), 16 (derecho de rectificación), 18 (derecho a la limitación del tratamiento) y 21 (derecho de oposición), siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

Por otra parte, el artículo 17 del RGPD, que regula el derecho al olvido, establece que este derecho no se aplicará cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública o con fines de investigación científica cuando el ejercicio del derecho imposibilite u obstaculice gravemente el logro de los objetivos.

El considerando 156 del RGPD justifica esas limitaciones diciendo que "*Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos*."

El considerando 69 RGPD hace referencia a la preeminencia del interés público sobre el interés privado y a la obligación del responsable del tratamiento de acreditarlo señalando que "*en los casos en que los datos personales puedan ser tratados*

lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado."

En suma, el RGPD parte de la base de que los derechos que otorga a los interesados (información, acceso, limitación, rectificación, oposición) no son ni el RGPD los concibe como unos derechos absolutos, sino que, muy al contrario, pueden ser objeto de limitación cuando se enfrenten a otros valores o bienes dignos de protección.

Nuestra legislación establece, por su parte, una serie de reglas respecto a la conservación de datos de salud, fundamentalmente por razones epidemiológicas y de investigación científica, que también suponen limitaciones a los derechos de los titulares de esos datos.

El artículo 29 del anteproyecto de nueva LOPD habilita al responsable del tratamiento, ante una petición de rectificación o supresión, al bloqueo de los datos y a conservarlos a disposición de las Administraciones públicas, Jueces y Tribunales, ministerio fiscal, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo debe procederse a la supresión.

El artículo 33 del Reglamento de la LOPD permite la denegación de los derechos de rectificación y cancelación en los siguientes supuestos:

> 1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.
> 2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

Respecto de la conservación de datos personales, la legislación sanitaria contiene una regulación específica. Dispone el artículo 17 LBAP que:

> 1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en 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.
>
> 2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

Por tanto, el paciente o los familiares del paciente fallecido no pueden exigir la supresión de sus datos de salud cuando pueda causarle un perjuicio o a un tercero o

cuando no haya transcurrido el plazo mínimo fijado por la legislación citada –cinco años-. Transcurrido ese plazo, los datos no se destruyen, sino que se bloquean según dispone el citado artículo 29 de la nueva LOPD, de modo que se conservarán únicamente a disposición de los Administraciones públicas y Jueces para la atención de posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas, así como por razones epidemiológicas y de investigación sanitaria.

10. Transferencias internacionales de datos de salud.

Propuesta normativa:

1. La transferencia de datos de salud con identificación de la persona a un tercer país u organización internacional solo podrá realizarse cuando concurra alguna de las siguientes circunstancias:

a) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
b) Cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate, garantizan un nivel de protección adecuado.
c) A falta de pronunciamiento de la Comisión, solo podrán realizarse transferencias de datos identificativos de la persona a un tercer país u organización internacional, cuando se obtenga autorización previa de la Autoridad de Control, que sólo podrá otorgarla si se obtienen garantías adecuadas, o cuando haya constancia fehaciente de que ofrezca un nivel adecuado de protección.
d) Cuando haya un riesgo grave e inminente para la salud de la población, con arreglo a las cláusulas contractuales tipo previstas en la Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país, o de lo que dispongan en lo sucesivo las Decisiones de la Comisión.

2. Los datos personales se tratarán conforme a lo dispuesto en el artículo 16 de la Decisión núm. 1082/2013/UE, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud.

3. El interesado debe ser advertido de que la transferencia de datos se realizará de conformidad con el Reglamento General de Protección de Datos y valiéndose de sistemas informáticos aportados por la Comisión.

Comentario exegético:

a) Transferencias internacionales.

El artículo 44 del RGPD sienta como principio general de las transferencias de datos personales a terceros países u organizaciones internacionales[72]:

> Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Y el artículo 45.1 del RGPD establece que:

> Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

Por su parte, el artículo 49 del RGPD prevé una serie de excepciones para situaciones específicas estableciendo que, en ausencia de una decisión de adecuación por la Comisión, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes: "a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas; d) la transferencia sea necesaria por razones importantes de interés público." Por tanto, es posible transferir datos de salud por razones epidemiológicas ante amenazas graves a la salud colectiva aun sin que la Comisión se haya pronunciado sobre la adecuación del país receptor para proteger los datos personales. Y, en efecto, el considerando 112 del RGPD contempla la necesaria transferencia de datos entre países en el concreto ámbito de la salud pública y las enfermedades contagiosas, pero señalando que, en ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional.

Como apunta MAYOR GÓMEZ[73], con estas medidas el RGPD trata de no menoscabar el nivel de protección de las personas físicas garantizado en la UE, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización

[72] Contempla la transferencia de datos a países u organizaciones fuera del espacio económico europeo. Las transferencias entre países pertenecientes a la UE se rigen, sin más, por el RGPD.

[73] MAYOR GÓMEZ, R., "Contenido y novedades del reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)" en revista GABILEX, núm. 6, JUNIO 2016, www.gabilex.jccm.es

internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. Con esta finalidad se encomienda a la Comisión la evaluación del nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país, y en el supuesto de que la Comisión no haya adoptado una decisión de adecuación sobre un territorio o sector, la transferencia de datos personales puede realizarse en casos especiales o cuando existan garantías apropiadas. Cuando un tercer país no garantiza un nivel de protección adecuado, se exige el bloqueo de determinadas transferencias. En definitiva, en ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado.

En nuestro Derecho positivo, una transferencia internacional de datos es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (artículos 33 y 34 de la LOPD y en el Título VI del RGPD y artículos 41 a 44 de la nueva LOPD). El exportador de datos es la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero. El importador de datos es la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargado del tratamiento o tercero.

Para realizar transferencias internacionales de datos, será necesaria la autorización previa de la Dirección de la Agencia Española de Protección de Datos en los supuestos establecidos en el artículo 43 del anteproyecto de la nueva LOPD.

b) Tratamiento de datos entre los Estados miembros de la UE frente a amenazas transfronterizas.

La Decisión núm. 1082/2013/UE, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud y por la que se deroga la Decisión núm. 2119/98/CE, establece normas sobre la vigilancia epidemiológica y el seguimiento de las amenazas transfronterizas graves para la salud, la alerta precoz en caso de tales amenazas y la lucha contra ellas, con inclusión de la planificación de la preparación y respuesta en relación con estas actividades, con el fin de coordinar y complementar las políticas nacionales. Tiene por objeto apoyar la cooperación y la coordinación entre los Estados miembros con el fin de mejorar la prevención y el control de la propagación de las enfermedades humanas graves a través de las fronteras de los Estados miembros y luchar contra otras amenazas transfronterizas graves para la salud, a fin de contribuir a alcanzar un nivel elevado de protección de la salud pública en la Unión. La Decisión crea una red de vigilancia epidemiológica de las enfermedades transmisibles y de los problemas sanitarios especiales. Respecto a la protección de datos personales, el artículo 16 establece:

> 1. En la aplicación de la presente Decisión, los datos personales se tratarán de conformidad con la Directiva 95/46/CE y el Reglamento (CE) no 45/2001. En particular,

se adoptarán las medidas técnicas y organizativas adecuadas para la protección de los datos personales contra la destrucción accidental o ilegal, la pérdida accidental, o el acceso no autorizado y contra cualquier otra forma de tratamiento ilícito.

2. El SAPR[74] incluirá una función de mensajería selectiva que permita comunicar los datos personales únicamente a las autoridades nacionales competentes implicadas en medidas de localización de contactos. Esa función de mensajería selectiva se concebirá y utilizará de manera que quede garantizada la seguridad y la legalidad del intercambio de datos personales.

3. Cuando las autoridades competentes que aplican las medidas de localización de contactos comuniquen datos personales necesarios a efectos de la mencionada localización a través del SAPR con arreglo al artículo 9, apartado 3, utilizarán la función de mensajería selectiva mencionada en el apartado 2 del presente artículo y comunicarán los datos únicamente a los demás Estados miembros que participen en tales medidas de localización.

4. Cuando transmitan la información indicada en el apartado 3, las autoridades competentes harán referencia a la alerta notificada previamente a través del SAPR.

5. Los mensajes que contengan datos personales se borrarán automáticamente de la función de mensajería selectiva 12 meses después de su envío.

6. Cuando una autoridad competente establezca que la notificación de datos personales realizada por ella con arreglo al artículo 9, apartado 3, ha resultado posteriormente contraria a la Directiva 95/46/CE por no haber sido necesaria para la aplicación de la medida de localización de contactos en cuestión, informará inmediatamente de ello a los Estados miembros destinatarios de la mencionada notificación.

7. Por lo que respecta a sus responsabilidades de notificación y rectificación de datos personales a través del SAPR, las autoridades competentes nacionales se considerarán responsables del tratamiento de conformidad con el artículo 2, letra d), de la Directiva 95/46/CE.

8. Por lo que respecta a sus responsabilidades de almacenamiento de datos personales, la Comisión será considerada responsable del tratamiento de conformidad con el artículo 2, letra d), del Reglamento (CE) no 45/2001.

Por otra parte, la Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, establece un conjunto de cláusulas contractuales tipo que prevé garantías adecuadas para la transferencia de datos a terceros países. Según esta Decisión, en ausencia de una normativa internacional en esta materia, las cláusulas contractuales tipo constituyen una herramienta de gran utilidad que permite transferir datos personales desde todos los Estados miembros con arreglo a un conjunto de normas comunes.

[74] Sistema de Alerta Precoz y Respuesta para la notificación de alertas a nivel de la Unión relacionadas con amenazas transfronterizas graves para la salud. El SAPR permitirá a la Comisión y las autoridades nacionales competentes mantenerse en comunicación permanente a efectos de alerta, evaluación de los riesgos para la salud pública y determinación de las medidas que pueden ser necesarias para proteger la salud pública (artículo 8.1 de la Decisión).

Respecto de las transferencias efectuadas a través de la red de vigilancia epidemiológica y de control de las enfermedades transmisibles, como ya conocemos, en la transmisión de la información epidemiológica es muy frecuente tener que trabajar con datos personalizados ya que la existencia de un brote epidemiológico puede requerir actuaciones concretas en una localidad o en una comarca, lo cual, a su vez, precisa de la identificación de los afectados.

11. Atribución a las autoridades de control de capacidad para autorizar la realización de estudios epidemiológicos.

Propuesta de regulación:

1. El comité de ética de investigación correspondiente, previamente a su realización, deberá autorizar los estudios de interés público en el ámbito de la salud pública en los que se traten datos masivos de salud con identificación de las personas sin obtener su consentimiento previo para el tratamiento.

2. Los responsables del tratamiento deberán elevar una consulta al comité de ética de investigación correspondiente a efectos de recabar su autorización previa.

Comentario exegético:

El considerando 89 del RGPD relata que la Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control, y que, pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales, por lo que estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces. Así, el artículo 36.5 RGPD dispone que:

> …el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Y el artículo 58.3. RGPD establece que

> "Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación: (…) c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa."

El artículo 57 del proyecto de nueva LOPD prevé esta facultad de autorización como una función de las Autoridades autonómicas de protección de datos. Entonces, en el caso de que lo disponga así nuestro legislador, los responsables del tratamiento de datos quedarían obligados a pedir autorización a esa Autoridad para tratar datos en una misión realizada en interés público en el ámbito de la salud pública. ¿Esa autorización es necesaria para cualquier actuación en salud pública o estudio epidemiológico? No

parece que deba ser así. Las actuaciones para la prevención de un riesgo o peligro grave para la salud de la población exigen inmediatez, respuestas rápidas, lo que resulta incompatible con la exigencia de obtener una autorización previa de una autoridad de control. En los estudios epidemiológicos, el artículo 16.3 de la LBAP obliga como regla general a asegurar el anonimato, y si se trabaja con datos anónimos sobra el control previo de la autoridad de control, pero ya hemos advertido que esta regla tiene muchas excepciones pues con frecuencia es preciso acceder a los datos personales para garantizar la solvencia del estudio. Por todo ello, en nuestro criterio, la autorización previa de la autoridad de control puede tener justificación para la realización de estudios de epidemiología que trate datos masivos y en los que no se trabaje con datos anonimizados sino con datos personalizados. Entendemos que la Autoridad autonómica en este caso deben ser los Comités de Ética de Investigación.

III. PROTECCIÓN DE DATOS DE SALUD EN EL ÁMBITO DE LA ASISTENCIA SANITARIA.

1. Encuadramiento en el marco del RGPD.

El artículo 9.2 del RGPD permite el tratamiento de datos de salud sin consentimiento del interesado cuando:

> h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros.

Y el artículo 9.3 añade:

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

Constatamos, pues, en primer lugar, que, como novedad, el RGPD incluye las prestaciones sociales y la gestión de los servicios sociales y, en segundo lugar, la trascendencia que el RGPD otorga al secreto profesional en el ámbito de la asistencia sanitaria y social.

2. Historia clínica electrónica unificada, interoperable, y módulos de especial custodia.

Propuesta de regulación.

1. Es finalidad principal de la historia clínica electrónica facilitar la asistencia sanitaria, y como finalidad complementaria posibilitar la investigación científica.

2. Los datos existentes en las historias clínicas son confidenciales, por lo que toda persona que elabore o tenga acceso a la información y a la documentación clínica está sujeta al deber de secreto. Igualmente, el personal de los centros y servicios sanitarios y sociosanitarios que acceda a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

3. La historia clínica electrónica unificada, bajo el principio de integrar toda aquella información que pueda ser relevante para la asistencia y la investigación, incorporará, además de la información correspondiente al contenido previsto en el artículo 15 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y deberes en materia de información y documentación clínica, la información generada en las actuaciones sanitarias derivadas de programas de salud pública y comunitaria.

Con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, la historia clínica deberá ser única mediante la identificación de toda la documentación clínica que concierne a la persona a través de un número único y excluyente para dicha persona, valedero para todo el Estado. Este número permitirá acceder a toda la documentación clínica generada tanto en la asistencia primaria como la especializada.

4. Se establecerán mecanismos que permitan determinar un módulo o módulos de información clínica que puedan contener datos considerados de especial custodia o intimidad en las áreas de genética, sexualidad y reproducción, psiquiatría, violencia doméstica, VIH y abortos. Los profesionales sanitarios asistenciales e investigadores que precisen acceder a los datos de módulos de especial custodia, serán advertidos por el sistema informático de esta circunstancia, con el fin de que indiquen el motivo del acceso y extremen la cautela en su manejo. En el registro de accesos quedarán singularizados los correspondientes a los datos de especial custodia, lo que permitirá realizar auditorías específicas.

5. Los servicios de salud de las comunidades cutónomas crearán un órgano que realizará de oficio auditorías de los accesos a las historias clínicas electrónicas de acuerdo con los protocolos establecidos al efecto.

6. No se podrán modificar automáticamente mediante aplicaciones informáticas los datos personales de las historias clínicas, particularmente las prescripciones de medicamentos, sin intervención del médico y sin el consentimiento del paciente.

Comentario exegético:

Conforme al art. 15 de la LBAP, "*la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente (...). La historia clínica tendrá como fin principal facilitar la asistencia*

sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud..."

En primer lugar, se trata de completar la regulación básica de la historia clínica hecha por la LBAP en cuanto herramienta fundamental de los profesionales de la salud tanto para la asistencia sanitaria como para la investigación científica y epidemiológica.

En segundo lugar, se trata de que exista un soporte único para cada persona con toda la información que le concierne sobre su salud, y hacer posible la interoperabilidad, esto es, el intercambio de la información clínica entre los diferentes agentes dentro del SNS, posibilitando el acceso a pacientes y profesionales, a la par que se garanticen la calidad de la asistencia y la confidencialidad e integridad de la información. La Historia Clínica Digital del Sistema Nacional de Salud es el instrumento idóneo. El Real Decreto 1093/2010, de 3 de septiembre, aprueba el conjunto mínimo de datos de los informes clínicos a intercambiar en el SNS y que viene a definir los datos imprescindibles que deben contener los informes clínicos de uso frecuente en el SNS, cualquiera que sea su soporte, electrónico o papel[75].

La obtención del consentimiento informado para prestar la asistencia sanitaria lleva implícito el consentimiento tanto para elaborar la historia clínica como para su posterior archivo en un registro pues la LBAP no exige, como es lógico, un consentimiento específico para su archivo. Ello por cuanto ha de entender que la historia clínica es un elemento inherente e imprescindible de la asistencia sanitaria prestada. La LBAP dice que el fin principal de la historia clínica es facilitar la asistencia sanitaria, de donde se infiere que el legislador está contemplando otros posibles fines, que son, obviamente, utilizar las historias para evaluar la calidad del centro sanitario, así como para hacer estudios epidemiológicos e investigación sanitaria. Y no cabe duda de que las historias clínicas son una fuente importante, no la única, para hacer investigación científica sanitaria, por lo que, en mi criterio, no está demás que así se exprese en la norma que defina el alcance de estos documentos electrónicos. Aunque, como ya hemos razonado anteriormente en el apartado dedicado a la investigación sanitaria, la explicitación de

[75] Un buen tratamiento de los datos de salud expresados en lenguaje médico-clínico exige su previa codificación de manera que permita traducir el lenguaje médico natural, de difícil tratamiento por la gran variabilidad en la expresión de sus conceptos, a otro normalizado que por su homogeneidad posibilita conocer la actividad de un centro sanitario y, lo que es más importante, la posibilidad de poder establecer la comparación entre ellos. Actualmente, promovido por la OMS, se utiliza el sistema CIE10ES (acrónimo de la Clasificación internacional de enfermedades, décima versión) como clasificación de referencia de codificación de la información clínica. Desde el 1 de enero de 2016 la clasificación CIE-10-ES (aprobada por el Consejo Interterritorial el 21 de marzo de 2013) es la clasificación de referencia para la codificación clínica y registro de morbilidad en España sustituyendo a CIE-9-MC. Las principales ventajas de la nueva clasificación derivan de su mayor precisión y adaptación al estado del arte actual en el ámbito clínico y las principales novedades residen en la flexibilidad, estandarización terminológica y mejoras metodológicas para una más adecuada codificación de los procedimientos. Los profesionales de la codificación son el **Técnico Superior en Documentación y Administración Sanitarias** (Real Decreto 768/2014, de 12 de septiembre) dependientes del Servicio de Admisión y Documentación Clínica: Unidad de Codificación. La codificación de datos en los centros sanitarios recae generalmente en los Técnicos Superiores en Documentación Sanitaria, si bien, siguen existiendo Administraciones autonómicas que en la Relación de Puestos de Trabajo de su Servicio de Salud no figura este puesto.

este fin no ha de conllevar necesariamente que el consentimiento prestado para recibir la asistencia sanitaria sirva para la posterior utilización de la historia con fines de investigación. Es más, en razón de la debilidad psicológica en la que se encuentra la persona enferma que busca alivio a sus dolencias y la superioridad psicológica del profesional sanitario que le atiende en la relación clínica que se crea, en la mayoría de los casos podría considerarse no válido un consentimiento expreso, obtenido a la par que el consentimiento para recibir asistencia sanitaria, para un eventual uso posterior de los datos con fines de investigación sanitaria, por faltar o estar muy disminuidos los elementos de libertad, conocimiento y conciencia por parte del enfermo. Recuérdese que el considerando 32 del RGPD señala que "*El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. (...) El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta*." Y que el considerando 43 añade "*Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento.*"

El tratamiento en el ámbito de la asistencia sanitaria, que se limita normalmente al acceso, consulta e incorporación de datos de salud, lo han de realizar los profesionales sanitarios (facultativos, personal de enfermería, etc.) vinculados asistencialmente con el paciente y con fines asistenciales y de medicina preventiva. Conforme al principio de proporcionalidad, la consulta de datos debe limitarse exclusivamente a los pertinentes para realizar el diagnóstico, la prestación de asistencia o el tratamiento sanitario, pues se entiende que los profesionales sanitarios vinculados asistencialmente con el paciente no tienen necesidad de acceder a cualquier dato de salud de la historia clínica electrónica para prestar una correcta asistencia.

Respecto de esta cuestión, es criterio del Grupo de trabajo del artículo 29 sobre el tratamiento de datos personales relativos a la salud en los historiales médicos

electrónicos (HME)[76], que "*Por lo que respecta a la presentación de los datos en los HME: el hecho de que sea posible distinguir entre diversas categorías de datos sanitarios que requieren grados muy distintos de confidencialidad sugiere que podría ser útil en general crear distintos módulos de datos en un sistema de HME con distintos requisitos de acceso. (...) Los datos particularmente sensibles podrían también protegerse mejor mediante su almacenamiento en módulos separados con condiciones de acceso especialmente estrictas. Como ejemplo cabe mencionar los datos sobre tratamientos psiquiátricos, VIH o abortos. En vez de excluir tales datos de un HME, lo que podría ser perjudicial para un correcto tratamiento médico futuro, deberían introducirse en el sistema restricciones especiales para el acceso a tales datos del HME, incluido el consentimiento explícito del paciente y barreras técnicas especiales (por ejemplo, "sobres sellados").*"

Asumiendo este criterio, el Decreto 29/2009, de 5 de febrero, de Galicia, sobre la historia clínica electrónica, norma pionera en este campo, estableció los "módulos de especial custodia" referidos a los datos más sensibles para una persona (datos sobre sexualidad, psiquiátricos, abortos, enfermedades infecciosas, etc.), que obligan al profesional a indicar el motivo de acceso a los mismos y que están sometidos a auditorías específicas. Una vez creado un módulo de acceso restringido, una cuestión a dilucidar es si su existencia debe enmascararse para que sea indetectable o, por el contrario, debe dotarse al sistema de un mensaje que advierta que existe información adicional pero que sólo está disponible en condiciones concretas. SÁNCHEZ CARO y GALLEGO RIESTRA[77] se inclinan por la segunda opción, habida cuenta de que el alcance e importancia de los antecedentes médicos de un paciente, esto es, qué datos son relevantes y cuáles no, es algo que sólo puede valorar el médico que le atiende en ese momento, quien, a la vista de una alerta sobre la existencia de más información en el sistema, puede también advertir al paciente de la conveniencia de que le autorice a consultarla.

Finalmente, el apartado 6 de la propuesta normativa trae causa de la sentencia del Tribunal Superior de Justicia del País Vasco, de 21 de febrero de 2017 -JUR/2017/116575-, que estimó el recurso interpuesto por el Consejo General de Colegios Oficiales de Médicos, contra la resolución de la Agencia Vasca de Protección de Datos, de 15 de abril de 2017, por la que se acordaba el archivo de la denuncia y las actuaciones practicadas en expediente sobre modificación de los datos personales de las historias clínicas por parte de Osakidetza, por la supuesta vulneración de la normativa de protección de datos al implantar la medida de sustituir automáticamente, a través de aplicaciones informáticas, ciertos tratamientos de marca comercial de medicamento por

[76] Documento de trabajo del Grupo de trabajo del artículo 29 sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), adoptado el 15 de febrero de 2007, p. 20.

[77] SÁNCHEZ CARO J. "La historia clínica electrónica gallega: Un paso importante en la gestión del conocimiento.", en *Derecho y Salud,* vol. 18, núm. 1, 2009, pp. 57-85; GALLEGO RIESTRA, S, "Historia clínica electrónica y derecho de autonomía del paciente: un conflicto de intereses", en *Papeles Médicos,* vol. 23, núm. 1, 2014, pp. 16-17.

denominación por principio activo. La sentencia acertadamente afirma que estos cambios de datos en la historia clínica, para ser acordes con la legislación de protección de datos, deben ser consentidos por el paciente titular de la historia.

3. Acceso a la historia clínica electrónica por los profesionales sanitarios.

Propuesta de regulación:

1. Los profesionales sanitarios que realizan el diagnóstico o el tratamiento del paciente tienen acceso directo e inmediato a las historias clínicas y a la información clínica incluida en las mismas en cumplimiento de sus funciones de prevención, de diagnóstico médico, de prestación de asistencia sanitaria o de tratamientos médicos, sin necesidad de requerir el previo consentimiento del paciente.

2. Los profesionales sanitarios que trabajen para las personas físicas o jurídicas que presten servicios concertados en hospitales privados o en otros centros sanitarios o sociosanitarios de otras comunidades autónomas, pueden acceder a la información contenida en la historia clínica electrónica del paciente al que deban prestar asistencia sanitaria. Este acceso estará limitado a las historias clínicas de los pacientes o usuarios que los centros sanitarios de los Servicios de Salud autonómicos remitan a dichos centros y en el marco temporal que dure esa atención. Los referidos profesionales incorporarán a la historia clínica electrónica la documentación clínica generada por la asistencia sanitaria prestada.

Comentario exegético.

El artículo 16.1 de la LBAP permite el acceso por los profesionales sanitarios que dan asistencia directa al paciente a su historia clínica sin necesidad de recabar su consentimiento previo. Se entiende que el consentimiento informado otorgado para recibir la asistencia sanitaria comprende también el consentimiento para acceder y tratar sus datos de salud a fines asistenciales. En concreto, el artículo 16.1 de la LBAP establece que los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

El artículo 9.2. h) del RGPD establece que los profesionales sanitarios que hagan medicina preventiva o laboral, diagnóstico y tratamiento directo de los pacientes, pueden acceder y tratar los datos de las historias clínicas sin necesidad de consentimiento explícito del paciente. Como contrapartida para garantizar la intimidad de los interesados y la reserva respecto de sus datos de salud, quedan sujetos al deber de secreto profesional, deber que se desarrolla ampliamente en la segunda parte de este informe.

Es un hecho muy frecuente que un mismo paciente sea atendido en distintos centros del Sistema Nacional de Salud, de titularidad pública o privada (concertado), bien por su

remisión por el servicio de salud a un centro concertado o bien por desplazamientos temporales a otras comunidades autónomas. Estas circunstancias no deben ser un impedimento u obstáculo para que los profesionales que deban prestarle asistencia accedan a su historia clínica. Así lo contempla y admite el artículo 10.5 del reglamento de desarrollo de la LOPD. Al objeto de hacer totalmente posible este acceso actualmente se está trabajando en el desarrollo de proyectos de interoperabilidad de los sistemas de historias clínicas electrónicas, incluso a nivel de la UE.

4. Acceso a la historia clínica para actividades de gestión, inspección, evaluación, acreditación y planificación de servicios sanitarios.

Propuesta de regulación:

1. El personal debidamente acreditado que ejerza funciones de gestión, inspección, evaluación, acreditación y planificación de servicios sanitarios, en la medida en que lo precise para el cumplimiento de sus funciones de gestión o de comprobación de la calidad y seguridad de la asistencia, del respeto de los derechos de los pacientes o de cualquier otro deber del centro con los pacientes o con la propia Administración sanitaria, podrá acceder a las historias clínicas. El acceso respetará el derecho a la intimidad de los pacientes.

2. El acceso con fines de gestión e inspección estará restringido a los datos imprescindibles para el ejercicio de sus funciones.

3. El acceso con fines de evaluación, acreditación y planificación, obliga a separar los datos de carácter cínico-asistencial de los datos personales, de manera que quede asegurado el anonimato.

Comentario exegético.

El artículo 9.2. h) e i) del RGPD prevé que el personal de gestión y administración de los centros y servicios sanitarios y sociales puede acceder conforme al principio de proporcionalidad a los datos de salud indispensables para el ejercicio de sus propias funciones, sin necesidad de consentimiento explícito del paciente.

La excepción también incluye el acceso a la información contenida en la historia clínica por el personal debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, en la medida en que lo precise para el cumplimiento de sus funciones de comprobación de la calidad y seguridad de la asistencia, del respeto de los derechos del paciente o usuario o de cualquier otro deber del centro en relación con los pacientes y usuarios. Pero cabe observar una diferencia sustancial: a) el personal de gestión (emisión de facturas, etc.) y el de inspección (inspección de concretas actuaciones clínicas) con frecuencia necesitan acceder a los datos identificativos de la persona titular de la historia clínica; b) el personal que realiza funciones generales de evaluación de la calidad y seguridad de la asistencia sanitaria de un centro sanitario, de

acreditación de centros o servicios, o que elabora programas o planifica actividades, que incluso puede ser realizado por empresas privadas (artículo 62 de la Ley de Cohesión y Calidad del Sistema Nacional de Salud), puede realizar perfectamente esas funciones manejando datos clínicos anonimizados.

5. Acceso a la receta médica electrónica y orden de dispensación hospitalaria.

Propuesta de regulación:

1. No será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica electrónica y orden de dispensación hospitalaria.

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

La información de la receta electrónica como fuente para la Base de Datos Clínicos de Atención Primaria no procederá de las oficinas de farmacia.

Comentario exegético:

La receta médica y las órdenes de dispensación hospitalarias son documentos normalizados que suponen un medio fundamental para la transmisión de información entre los profesionales sanitarios, además de su papel como soporte para la gestión y facturación de la prestación farmacéutica que reciben los usuarios del Sistema Nacional de Salud.

Las funciones de colaboración de las Oficinas de farmacia con el Sistema Nacional de Salud y con los órganos competentes en materia sanitaria en cada una de las Comunidades Autónomas son asumidas por los Colegios Oficiales de Farmacéuticos y por el Consejo General mediante Concierto, y el informe de la AEPD 126/03 concluye que las actuaciones que el Concierto exige de los Colegios Profesionales en relación al tratamiento automatizado de datos personales contenidos en las recetas, constituye un supuesto de cesión de datos entre Administraciones públicas (art. 21 LOPD).

Establece el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación hospitalaria (artículos 11 y 19.2), que no será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico. Como contrapunto también establece que en los trámites a que sean sometidas las recetas médicas y órdenes de dispensación hospitalaria, y especialmente en su tratamiento informático, así como en su proceso electrónico, deberá

quedar garantizada, conforme previene la normativa específica de aplicación, la confidencialidad de la asistencia médica y farmacéutica, la intimidad personal y familiar de los ciudadanos y la protección de sus datos de carácter personal. Para garantizar dichos niveles de seguridad, esta información sólo será accesible desde la oficina de farmacia a efectos de dispensación, residirá de forma permanente en los sistemas de receta electrónica gestionados por las Administraciones sanitarias y no podrá ser almacenada en los repositorios o servidores ajenos a estas, establecidos para efectuar la facturación, una vez esta se haya producido.

6. Consentimiento para el tratamiento de datos de salud de menores de edad y acceso a sus datos.

Propuesta de regulación:

1. Corresponde a las personas con catorce años cumplidos otorgar el consentimiento para procederse al tratamiento de sus datos de salud. En el caso de los menores de trece años se requerirá el consentimiento de los padres o tutores.

Los padres o quien ostente la patria potestad podrán acceder también a los datos de salud del menor al objeto de poder velar adecuadamente de su salud.

2. El menor de edad con catorce años cumplidos tendrá acceso a sus datos de salud.

Comentario exegético.

El artículo 8 RGPD dispone que el consentimiento para el tratamiento de datos lo deberán dar los niños cuando tengan como mínimo 16 años, y si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó, añadiendo que el responsable del tratamiento hará esfuerzos razonables para verificar que el consentimiento ha sido dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible. No obstante, permite a los Estados miembros que puedan establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

Para el ámbito de la protección de datos personales en nuestro país se ha estimado tradicionalmente que los mayores de catorce años tienen madurez suficiente para otorgar su consentimiento para el tratamiento de sus datos personales, así como para ejercitar derechos respecto de ese tratamiento. En concordancia con este criterio doctrinal, establece el artículo 13 del Real Decreto 1720/2007, por el que se aprueba el Reglamento de la LOPD sobre el consentimiento para el tratamiento de datos de menores de edad lo siguiente:

> 1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su

> prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

Este es, además, el criterio mantenido por la Agencia Española de Protección de Datos Personales desde su informe 409/2004, basándose en el artículo 162.1 del Código Civil, que excluye de la representación legal de la patria potestad los actos relativos a los derechos de personalidad u otros que el hijo, de acuerdo con las leyes y sus condiciones de madurez, pueda realizar por sí mismo. La regla general establecida por la Agencia Española de Protección de Datos es que el menor a partir de los 14 años puede ejercer por sí sólo el derecho de acceso a los datos de su historia clínica, sin perjuicio de que los padres que ostentan la patria potestad también puedan acceder a estos datos en el ejercicio inherente de los deberes de la patria potestad. Y es que el artículo 154 del Código Civil permite implícitamente que se disponga de la información sanitaria de los hijos para poder velar adecuadamente por su salud. De ahí que se posibilite la cesión de dicha información a quienes ostenten la patria potestad.

La LBAP no contiene ninguna referencia respecto de la autorización para el tratamiento y el acceso del menor de edad a sus datos clínicos.

Se trata ahora, por exigirlo así el RGPD, de elevar esta determinación reglamentaria a rango de Ley para el ámbito de los datos de salud.

7. Conservación de la documentación clínica.

Propuesta de regulación:

1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en 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.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación procesal vigente. Se conservará, asimismo, por razones epidemiológicas, de salud pública, investigación, inspección y evaluación, procediéndose, como regla general, a la disociación de los datos.

3. La cancelación de datos a instancia del interesado dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de estas. Cumplido el citado plazo deberá procederse a la supresión.

Comentario exegético:

Los datos de salud deben ser cancelados cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido recabados y registrados, que en su inmensa mayoría son fines directamente asistenciales. La LBAP fija un plazo mínimo de 5 años desde el alta del paciente para la conservación de las historias clínicas, plazo que algunas comunidades autónomas han incrementado notablemente (por ejemplo, Cataluña, 10 años desde la última asistencia), o incluso declarándola indefinida a criterio del facultativo (Cantabria, Castilla y León, Cataluña, etc.). Ahora bien, no cabe duda de que existen, además de los asistenciales, otros fines que justifican la conservación de los datos de salud, aun en contra la voluntad de su titular, como los son los fines judiciales (exigencias de responsabilidad penal o civil), epidemiológicos, de investigación científica y de gestión sanitaria.

En suma, respecto de los plazos de conservación es necesario diferenciar a) fin asistencial, que, con un plazo mínimo de cinco años desde la última asistencia, queda a la discrecionalidad técnica de los profesionales sanitarios; b) fin de investigación, para la que la conservación podrá ser personalizada o anonimizada; c) fin judicial, en el que la conservación será como mínimos mientras no prescriban las acciones judiciales pertinentes; fines epidemiológicos y de salud pública, inspección y evaluación, sin tope de tiempo pero con la condición de que se proceda la disociación de los datos.

El artículo 5 del RLOPD define la cancelación como el procedimiento en virtud del cual el responsable cesa en el uso de los datos. Añade que la cancelación implica el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades, y que transcurrido ese plazo deberá procederse a la supresión de los datos.

8. Instalación de cámaras de videovigilancia por razones de seguridad en consultas y otros espacios asistenciales.

Propuesta de regulación:

1. Con el objeto de prevenir posibles agresiones a los profesionales sanitarios por parte de los pacientes, podrán instalarse cámaras de videovigilancia en las consultas y otros espacios en los que se asista a pacientes, sin necesidad de obtener su previo consentimiento, siempre que se preserve convenientemente la privacidad e intimidad de los mismos. A estos efectos, serán medidas mínimas las siguientes: las cámaras podrán grabar la imagen, pero no la voz; no podrá captarse imágenes con pacientes desnudos ni de documentos u otros medios desde los que puedan conocerse datos clínicos del paciente.

2. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

3. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible que identifique, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

Comentario exegético:

La instalación de cámaras de videovigilancia en la consulta médica implica, de entrada, una invasión de la privacidad e intimidad de la persona en un ámbito como es el de la asistencia sanitaria donde la intimidad del paciente es prioridad máxima.

La Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos[78], sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, razona en su expositivo lo siguiente:

> La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático. Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 1.4 del Real Decreto 1322/1994 de 20 de junio, que considera como dato de carácter personal la información gráfica o fotográfica. En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales. En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

Pues bien, el proyecto de la nueva LOPD en su artículo 22 habilita a utilizar videocámaras para preservar la seguridad de las personas:

> Artículo 15. Tratamientos con fines de videovigilancia.
> 1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.
> (…)

[78] BOE de 12 de diciembre de 2006.

> 3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.
> No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 29.
> 4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
> En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

No parece que haya dudas de que, ante el progresivo aumento de agresiones a profesionales sanitarios, algunas de ellas con graves lesiones físicas a los mismos, la instalación de cámaras de videovigilancia con las debidas precauciones y medidas para garantizar la intimidad del paciente y, particularmente, todo lo relativos a su enfermedad o dolencia y a los datos personales que se hacen manifiestos durante la consulta, es una medida proporcional al fin perseguido. Hay consenso entre los juristas[79] en que la instalación debería hacerse de forma que se graben las imágenes, pero no la voz, que la cámara no esté orientada hacia lugares en los que el paciente se desnuda o se somete a exploraciones de partes íntimas de su cuerpo, que la cámara no permita captar documentos o pruebas médicas, etc. Cumpliendo estas concretas condiciones más el resto de obligaciones formales que se establecen en la Instrucción 1/2006, de la Agencia Española de Protección de Datos, es plausible la legitimidad de la instalación de las cámaras de videovigilancia.

IV. DELEGADO DE PROTECCIÓN DE DATOS.

Propuesta de regulación:

Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos para cada uno de los centros sanitarios legalmente obligados al archivo y mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, así como para los archivos que integran el Sistema de Información en Salud pública.

Comentario exegético:

Los datos de salud se contienen fundamentalmente en las historias clínicas electrónicas y en papel archivadas en los centros hospitalarios y de atención primaria, si bien la informatización y unificación de las historias clínicas de cada paciente está ya muy

[79] Véase ARROYO, J., ¿Se pueden instalar cámaras de seguridad en la consulta del médico?, Redacción Médica de 3 de junio de 2017. Disponible en https://www.redaccionmedica.com/secciones/derecho/-se-pueden-instalar-camaras-de-seguridad-en-la-consulta-del-medico--2352.

avanzada. A estos registros han de sumarse los archivos que se integran en el Sistema de Información en Salud Pública constituido por los sistemas de información e materia de salud pública creados y gestionados por los responsables de salud pública de las Comunidades Autónomas. Todos estos archivos y ficheros contienen cantidades ingentes de datos de salud.

Pues bien, es obligado contar con profesionales de la privacidad, que el artículo 37 RGPD denomina "delegado de protección de datos"[80], cuando el tratamiento lo lleve a cabo una autoridad u organismo público y cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 RGPD, esto es, de datos de salud. Se considera que el archivo informatizado de historias clínicas de un hospital es de por sí un tratamiento a gran escala. En efecto, el Grupo de Trabajo del artículo 29 en las Directrices sobre Delegados de Protección de Datos, aprobadas el 13 de diciembre de 2016, afirma que el tratamiento de datos de pacientes en el desarrollo de la actividad de un hospital es un tratamiento a gran escala. Lo es también, por supuesto, el tratamiento de datos de salud del Sistema de Información en Salud Pública.

El artículo 37 RGPD garantiza la profesionalidad del delegado al disponer que será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho, a la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que le competen. Interesa resaltar el perfil eminentemente jurídico que el RGPD otorga a esta nueva figura muy acorde con su función de proteger un derecho fundamental. Puede formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios. El responsable o el encargado del tratamiento han de hacer públicos los datos de contacto del delegado de protección de datos y han de comunicarlos a la autoridad de control.

Por su parte, el artículo 38 RGPD fija la posición del delgado de protección de datos al exigir que el responsable y el encargado del tratamiento garanticen que participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, respaldándole y facilitándole los recursos necesarios para el pleno y adecuado desempeño de sus funciones, para el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados. Procura preservar su total independencia al exigir del responsable y encargado que garanticen que no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones, de modo que no puede ser destituido ni sancionado por estos por el desempeño de sus funciones. El delegado de protección de datos debe rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado. También

[80] Sobre esta nueva figura véase MARTÍNEZ MARTÍNEZ, R., "El rol de los profesionales de la privacidad", en el libro colectivo *Hacia un nuevo Derecho Europeo de Protección de Datos,* Tirant lo Blanch, 2015, pp. 539-570. Véase también la Directriz (WP243, de 13 de diciembre de 2016) elaborada por el Grupo de Trabajo del artículo 29.

dispone que los interesados puedan contactar con el delegado de protección de datos respecto de todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del RGPD. Finalmente, le impone la obligación de mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

El artículo 39 RGPD le atribuye las siguientes funciones: a) información y asesoramiento a las personas que se ocupen del tratamiento de sus obligaciones; b) supervisión del cumplimiento de lo dispuesto en el RGPD y en el derecho complementario del Estado miembro, así como de la concienciación y formación del personal; c) asesoramiento acerca de la evaluación del impacto de las operaciones de tratamiento; d) cooperación con la autoridad de control.

El artículo 35.1. apartado l), del anteproyecto de la nueva LOPD establece que deberá existir un delegado de protección de datos en los centros sanitarios legalmente obligados al mantenimiento de historias clínicas de los pacientes con arreglo a lo dispuesto en la LBAP. Se ha escrito que, atendiendo al número de hospitales y centros de atención primaria existentes en España, harán falta 3.836 delegados (788 para los hospitales y 3.048 para los centros de salud), si bien un delegado podrá atender a uno o varios hospitales o centros de salud, dependiendo del tamaño, por lo que estas estimaciones varían en función del organigrama de cada institución sanitaria[81]. Sin embargo, considerando la muy avanzada unificación de la historia clínica de cada paciente (primaria y especializada) y que el depósito y mantenimiento de los datos de salud recae en los Servicios de Admisión y Documentación Clínica, que generalmente se ubican en los hospitales o complejos hospitalarios, no en los centros de salud, este número se reduciría significativamente.

V. ACCESOS A FICHEROS DE DATOS DE SALUD Y POSIBILIDAD DE QUE EL INTERESADO CONOZCA TODOS LOS ACCESOS EFECTUADOS.

Propuesta de regulación:

1. De cada intento de acceso a un fichero o tratamiento automatizado de datos de salud se guardarán, como mínimo, 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. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

[81] ALCALAL C. y HUERTAS J., España obliga a que en 10 meses cada hospital tenga un agente de datos. Redacción Médica, 13 de julio de 2017.
Disponible en https://www.redaccionmedica.com/secciones/derecho/justicia-obliga-a-que-en-10-meses-cada-hospital-tenga-un-agente-de-datos-4893.
.

2. Toda persona tiene derecho a conocer en todo caso quién ha accedido a sus datos de salud, el motivo del acceso y el uso que se ha hecho de ellos, salvo en caso de uso codificado de los mismos.

Comentario exegético:

Con el objeto de controlar los accesos a los datos de salud por terceras personas, cuestión muy preocupante particularmente cuando se trata de historias clínicas electrónicas, el artículo 103 del RLOPD establece:

> De cada intento de acceso se guardarán, como mínimo, 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. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Debe existir, por tanto, un registro de accesos, que ha de conservarse, al menos, durante dos años. La AEPD, interpretando el artículo 103, señala en su informe 584/2009 que "El aspecto esencial a tener en consideración en estos casos será el que la información almacenada en el registro de accesos permita identificar inequívocamente qué persona ha tenido acceso y a qué información contenida en el fichero en cada momento, a fin de que, en caso de ser necesario reconstruir cuándo y cómo se produjo una determinada revelación de un dato, sea posible identificar la persona que pudo conocerlo en ese momento concreto."

En suma, el control de los accesos debe efectuarse de la forma más detallada posible, a fin de conocer efectivamente quién ha podido en cada momento conocer los datos incorporados al sistema, es decir, a qué datos o recursos se ha accedido, sin que puedan efectuarse meros controles genéricos, por referencia al sistema en conjunto. Por consiguiente, el responsable del fichero debe contar con las aplicaciones informáticas necesarias que permitan cumplir con las exigencias establecidas en el artículo 103 del RLOPD.

No es necesario registrar los accesos cuando el responsable del fichero es una persona física y garantiza que únicamente él tiene acceso y trata los datos de salud. Esta excepción es particularmente aplicable a los médicos con consulta privada.

El artículo 15.1 de la todavía vigente LOPD, establece que el interesado tiene 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. Es decir, solo a sus propios datos, no a datos atinentes a terceras personas.

La AEPD, apoyándose en el citado artículo 15.1 reiteradamente se ha pronunciado en contra de que el titular de los datos pueda conocer las personas que han accedido a sus datos (Informe 167/2005; Informe 171/2008; resolución R/00948/2011; resolución

R/00945/2013; resolución R/02488/2015, entre otras). Razona que el derecho concedido al interesado por la LOPD únicamente abarca 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. Justifica este aserto señalando que esos datos serían datos de carácter personal, que deberían contar con su consentimiento, o encontrarse habilitada por ley la posibilidad, lo que no sucede dado el alcance que el artículo 15.1 de la LOPD otorga al derecho de acceso (Informe 167/2005). La resolución R/00945/2013 fue recurrida ante la Audiencia Nacional, recurso cuyo conocimiento correspondió a la sección 1ª de la Sala de lo Contencioso-administrativo, que rechazó las pretensiones de la recurrente en sentencia 26 de febrero de 2014 confirmando la interpretación de la AEPD.

Siguiendo este criterio, el artículo 19.2 del Decreto 24/2011, de 12 de abril, de la documentación sanitaria en Castilla-La Mancha, establece que "El derecho de acceso del paciente a los datos de su historia clínica no comprende la información sobre los datos personales de las personas que, dentro del ámbito de organización del responsable del fichero, han podido tener acceso a la misma en el ejercicio de sus funciones."

No obstante, en la normativa autonómica encontramos posiciones contrarias. Así, el artículo 31.1 de la Ley Foral 17/2010, de 8 de noviembre, sienta el derecho "a conocer en todo caso quién ha accedido a sus datos sanitarios, el motivo del acceso y el uso que se ha hecho de ellos, salvo en caso de uso codificado de los mismos". El derecho se extiende, por tanto, a conocer no solo sus propios datos de salud, sino a conocer también las personas que han accedido a esos datos.

La mejor doctrina se inclina mayoritariamente por que se permita al interesado el conocimiento de las personas que han accedido a sus datos de salud[82]. En cualquier caso, reconocer el derecho a conocer las personas que han accedido a los datos de salud no es una cuestión pacífica.

En nuestro criterio, la solución más acertada para esta cuestión pasa por permitir el conocimiento por el interesado de las personas que han accedido s sus datos, lo que, como afirma la AEPD, requiere de una norma de rango legal que así lo prevea. De ahí la propuesta que hacemos en este apartado.

VI. REGISTROS DE EFECTOS ADVERSOS Y PROTECCIÓN DE DATOS DE SALUD.

Propuesta de regulación:

1. En la comunicación de efectos adversos al correspondiente registro se identificará al paciente o pacientes que los han sufrido y el centro sanitario donde se ha producido.

[82] Véase al respecto, GALLEGO RIESTRA, S. y RIAÑO GALÁN, I., "¿Tiene el paciente derecho a saber quiénes y por qué han accedido a su historia clínica?, *Revista Derecho y Salud,* volumen 22, núm. 1, 2012, pp. 85-96.

No será aplicable el derecho de acceso establecido en el artículo 15 del Reglamento (UE) 2016/679, de 27 de abril de 2016, por parte del paciente a los datos personales que le conciernen existentes en los registros de efectos adversos.

2. Los profesionales sanitarios encargados del estudio, tratamiento y análisis de los datos obrantes en los registros de efectos adversos, se acomodarán al siguiente estatuto:

a) Quedan sujetos al deber de secreto profesional. Este deber cederá exclusivamente respecto de aquellos datos relevantes que tengan que ser utilizados en un proceso penal siempre y cuando el órgano judicial competente decida previamente que los mismos constituyen indicios de la comisión de un delito que no podrían obtenerse por ningún otro medio.

b) Cuando deban actuar como perito o testigo en un proceso judicial penal, manifestará razonadamente al juez o tribunal su deber de guardar secreto respecto de hechos por los que se le interrogue, y el órgano judicial considerando el fundamento de la negativa a declarar y ponderando el deber legal de secreto profesional frente al derecho a obtener una protección jurídica efectiva de las partes, resolverá, mediante providencia, lo que proceda en derecho. Si el testigo quedare liberado de responder, se hará constar así en el acta.

c) No están obligados a denunciar los delitos públicos que puedan apreciar por el conocimiento y estudio de los efectos adversos comunicados[83].

Comentario exegético:

El artículo 59 de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del SNS dispone la creación de una infraestructura de calidad que contenga como uno de sus elementos integrantes un registro de acontecimientos adversos, que recoja información sobre aquellas prácticas que hayan resultado un problema potencial de seguridad para el paciente, y en su artículo 60 hace responsable de esta infraestructura de calidad a la Agencia de Calidad del Sistema Nacional de Salud, que estará a disposición del Ministerio de Sanidad, Servicios Sociales e Igualdad y de la comunidades autónomas[84]. El Ministerio de Sanidad, Servicios Sociales e Igualdad, creó en el año 2010 el Sistema de Notificación y Aprendizaje para la Seguridad del Paciente (SiNASP) con el objetivo de mejorar la seguridad de los pacientes a partir del análisis de situaciones, problemas e

[83] Esta determinación obligaría a modificar el artículo 263 de la ley de Enjuiciamiento Criminal, que incluiría a los profesionales sanitarios, junto a los abogados y eclesiásticos, en la exención a la obligación de denunciar delitos públicos. Se trataría de una exención parcial relativa a los registros de efectos adversos.

[84] Sobre la puesta en funcionamiento de estos registros, URRUELA MORA, A., "Los sistemas de notificación y registro de eventos adversos en la esfera sanitaria. Aspectos técnicos y legales relacionados con su puesta en funcionamiento en España", en el libro colectivo *Derecho Sanitario y Bioética,* Tirant lo Blanch, 2011, pp. 335-361.

incidentes que produjeron, o podrían haber producido, daño a los pacientes. La notificación es voluntaria, si bien anima a los profesionales a utilizar el sistema, colaborando así en el aprendizaje y la mejora de la seguridad del paciente. La notificación es anónima o nominativa con anonimización posterior. El SiNASP está disponible para hospitales y para centros de Atención Primaria. El sistema tiene un nivel local en el propio centro donde se hace la gestión y análisis del efecto adverso comunicado, y un nivel supralocal de agregación de las notificaciones en el ámbito de la Comunidad Autónoma y posteriormente en el SNS. Sólo los profesionales de los centros que están dados de alta en el sistema pueden notificar incidentes. Actualmente, utilizan este sistema nueve comunidades autónomas.

Por otra parte, las comunidades autónomas han creado diversos registros de efectos adversos, si bien limitados a determinadas especialidades médicas o a concretas prestaciones sanitarias[85].

La comunicación de datos a registros de efectos adversos es obligatoria en el caso de la farmacovigilancia (efectos adversos de medicamentos) y de los ensayos clínicos[86].

Salvo estos supuestos, se echa en falta una norma que, con carácter general, regule el régimen de los registros de efectos adversos estableciendo las garantías necesarias, en particular en lo atinente al deber de secreto y a la protección de los datos de salud del afectado por el efecto adverso. En la política de vacunación es muy importante el buen funcionamiento de un registro de efectos adversos. Aquí hay una oportunidad para cubrir esta laguna legal.

Con la creación y funcionamiento de los registros de efectos adversos no se trata de culpabilizar a los profesionales sanitarios, sino de analizar las causas que los han producido a efectos de evitarlos en el futuro. Es indispensable que los profesionales sanitarios estén seguros de este enfoque de los registros para que colaboren, y para ello, entre otras cosas, es necesario disponer de una normativa que excluya potenciales exigencias de responsabilidad por esta vía.

Acudiendo al derecho comparado, comprobamos que, actualmente, existen tres sistemas en lo que hace a la protección de los datos del paciente cuando se comunican efectos adversos[87]. La mayoría prohíben la identificación del paciente a través de los datos que se suministran. Otros sistemas (Nueva Zelanda, Australia) obligan a la identificación del

[85] Por ejemplo, por Orden Foral 48/2016, de 3 de junio, del Consejero de Salud de Navarra, se crea y regula el registro de sospechas de reacciones adversas a medicamentos.

[86] En el ámbito de la farmacovigilancia la comunicación es obligatoria conforme dispone el artículo 53.2 del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios. Igualmente, en el caso de los ensayos clínicos es obligatoria la comunicación conforme disponen los artículos 49 y 50 del Real Decreto 1090/2015, de 4 de diciembre, de ensayos clínicos con medicamentos.

[87] Datos obtenidos del trabajo de LARIOS RISCO, D. y LOMAS HERNANDEZ, V., "Aprendizaje a partir del error: requerimientos jurídicos de un registro nacional de efectos adversos en el SNS, en *Derecho y Salud,* vol. 20, núm. 1, 2010, pp. 10-11.

paciente. Un sistema mixto (Dinamarca, Finlandia, Suecia) exige la identificación del paciente, pero prohíbe su utilización por parte de terceros ajenos al sistema.

En nuestro país, la doctrina se manifiesta dividida. Un sector apoya la no identificación del paciente[88]. Ahora bien, a pesar de que el sistema se base en el carácter anónimo de la notificación, los profesionales del registro encargados del análisis de las causas raíz del efecto adverso a nivel de centro sanitario, pueden llegar a conocer con facilidad en un número significativo de casos la identidad de los intervinientes -profesionales sanitarios y pacientes-[89]. Otro sector doctrinal se inclina por el sistema mixto ya que reporta más beneficios al registro de efectos adversos[90]. En cualquier caso, se opte o no por un sistema anónimo, la posibilidad de identificar al paciente es bastante alta. De optar por el sistema mixto, la comunicación de los efectos adversos sería identificando al paciente, si bien a este no le sería aplicable el derecho de acceso establecido en el artículo 15 del RGPD, a los datos personales que le conciernen existentes en los registros de efectos adversos. Ello no es óbice para que el paciente deba ser inmediatamente informado de la existencia de un efecto adverso no deseado y se deje constancia en su historia clínica, pues esta es una obligación del médico responsable derivada de la LBAP que ha de cumplimentar en el marco de la relación clínica con el paciente. Así pues, en todo caso el paciente debe saber del efecto adverso por un cauce distinto al de su comunicación al registro de efectos adversos y, en su caso, reclamar por esa vía ordinaria.

Respecto al régimen de los registros de efectos adversos, la generalidad de la doctrina [91] se inclina por considerar que para que un sistema de registro de efectos adversos tenga éxito en nuestro país, esto es, sea bienvenido por los profesionales sanitarios y sistemáticamente comuniquen los errores cometidos y los efectos adversos producidos no deseados, en suma, para que cumpla el objetivo por el que se instaura, debe estar presidido por los siguientes criterios: a) voluntariedad de las comunicaciones, ello sin perjuicio de la obligatoriedad en determinados sectores o ámbitos conforme establezca la legislación específica; b) carácter no punitivo, esto es, la indemnidad de los

[88] Esta es una de las conclusiones del informe "*El establecimiento de un sistema nacional de notificación y registro de incidentes y eventos adversos en el sector sanitario: aspectos legales*", (ROMEO CASABONA, C. Y URRUELA MORAL, A. -directores-), Informes, Estudios e Investigación, Ministerio de Sanidad y Política Social, 2009, p. 96: "La experiencia en otros estados revela la paulatina asunción de apuestas, decididas y ambiciosas, en favor de sistemas de comunicación de eventos adversos en el ámbito sanitario, los cuales configuran una variedad de modelos merecedores de estudio, y al mismo tiempo demuestra que las claves de los mismos radican en diversos rasgos predominantes, como son su carácter no punitivo, así como su orientación exclusiva a la formación de los profesionales sanitarios y a la prevención de errores. Por ello, su diseño con arreglo a un principio estricto de confidencialidad garantizado y el carácter anónimo de los datos así almacenados resulta, a nuestro entender, fundamental."

[89] Seguimos el informe citado en nota anterior, p. 93.

[90] LARIOS RISCO, D. y LOMAS HERNANDEZ, V, cit., pp. 1-32.

[91] Véase *El establecimiento de un sistema nacional de notificación y registro de incidentes y eventos adversos en el sector sanitario: aspectos legales*, Informes, Estudios e Investigación, (ROMEO CASABONA, C. Y URRUELA MORA, A.-directores-), Ministerio de Sanidad y Política Social, 2009; MARTÍN DELGADO, Mª C., CABRÉ PERICAS, L., "Aspectos éticos y legales sobre la seguridad del paciente" en *Revista de Bioética y Derecho,* núm. 15, 2009, pp. 6-14; LARIOS RISCO, D. y LOMAS HERNANDEZ, V., "Aprendizaje a partir del error: requerimientos jurídicos de un registro nacional de efectos adversos en el SNS, en *Derecho y Salud,* vol. 20, núm. 1, 2010, pp. 1-42.

profesionales sanitarios implicados como base de la confianza de los mismos; c) derecho a la intimidad de los sujetos implicados; d) deber de secreto profesional de los sujetos responsables del estudio, análisis y tratamiento de los datos del registro de efectos adversos.

Otros aspectos atinentes a los profesionales sanitarios involucrados en los efectos adversos o que los comunican a los registros, particularmente lo relativo a la indemnidad, necesitados de urgente regulación podría ajustarse a los siguientes criterios (que no expresamos en la propuesta de regulación por cuanto una ley reguladora de la protección de datos de salud no es lugar adecuado para la misma):

- Como regla general, la comunicación por los profesionales sanitarios o las instituciones que han causado el daño debe ser voluntaria, con excepción de aquellos ámbitos en los que la normativa específica establezca la obligatoriedad de la comunicación.

- El profesional sanitario que lleve a cabo una comunicación no puede ser sometido a resultas de la misma a investigación disciplinaria o a sanciones por parte de la autoridad donde desempeña su labor profesional.

- Los datos registrados no deben ser utilizados en ningún caso en los procesos civiles y contencioso-administrativos como medio de prueba de eventuales infracciones de la *lex artis* por parte de los profesionales implicados, ni deben servir de soporte para la interposición de reclamaciones o denuncias contra dichos profesionales, que deberán seguir su cauce normal.

- Cuando el comunicante o denunciante de un efecto adverso sea un profesional o una persona distinta al profesional que ha causado el daño, debería poder hacer la comunicación o denuncia de forma anónima. Cuando opte por hacer una comunicación nominativa ha de poder ejercer el derecho de oposición a que se proceda al tratamiento de sus datos personales identificativos.

VII. CARPETA PERSONAL DE SALUD. ACCESO Y PROTECCIÓN DE LOS DATOS CONTENIDOS EN LA CARPETA PERSONAL DE SALUD.

Propuesta de regulación:

1. La carpeta personal de salud constituye un espacio de almacenamiento personal de información, creado por los sistemas públicos de salud de las comunidades autónomas, a petición de la persona, que se mantendrá activo bajo su responsabilidad o de la persona por ella autorizada.

2. El acceso a la carpeta personal de salud se efectuará a través de medios electrónicos, como el certificado digital, el DNI u otros mecanismos de autenticación

aplicables según la vigente normativa de administración electrónica, gestionados por el correspondiente servicio de salud autonómico.

3. Podrán acceder a la carpeta personal de salud:

a) La propia persona usuaria cuando haya cumplido 14 años de edad.

b) Cuando se trate de personas menores de 14 años, podrán acceder a su carpeta personal su padre, madre o tutor legal.

c) Cuando se trate de personas incapacitadas, podrá acceder a su carpeta su representante legal o la persona autorizada expresamente por el representante legal.

d) Cuando se trate de personas mayores de edad que, no estando incapacitadas judicialmente, sean pacientes crónicos y con limitaciones propias de la edad o de la enfermedad, podrá acceder a su carpeta la persona autorizada expresamente por la misma.

4. Los datos de carácter personal que se faciliten quedarán registrados en un fichero de titularidad del servicio de salud autonómico respetivo.

5. La persona capacitada para el acceso a la carpeta conforme al apartado 3 de este artículo podrá ejercer los derechos de rectificación, cancelación y oposición ante el servicio de salud autonómico correspondiente, solicitando por escrito y acreditando fehacientemente su identidad o la representación que ostente, de conformidad con la normativa vigente.

Comentario exegético:

La carpeta personal de salud es un instrumento nuevo generado en el campo de las tecnologías de la información sanitaria, que nace como un espacio de almacenamiento personal de información de salud incorporada por la propia persona usuaria, además de la generada por dispositivos y aplicativos relacionados con la salud, de autocontrol del estado físico, generada a iniciativa de los servicios autonómicos de salud.

Ofrece a los pacientes acceso a su información médica, servicios como la programación de citas, o comunicación entre los miembros del equipo de atención de salud y el paciente. También permite al propio paciente registrar datos de salud escribiéndolos directamente o recogidos desde aparatos de vigilancia y monitorización domésticos, por lo que constituye un instrumento de gran utilidad para la gestión de la enfermedad crónica y para la prevención y promoción de la salud. En suma, se trata de ofrecer a la ciudadanía un entorno personalizado que le permite consultar de forma privada y segura sus datos clínicos, realizar gestiones y trámites diversos, así como consultar información de interés como farmacias de guardia, buscador de centros sanitarios, etc. Es un soporte digital independiente y completamente diferenciado de la historia clínica electrónica.

Se ha apuntado[92] el tremendo potencial de las carpetas personales de salud para redefinir el modelo de salud, transformar la relación entre las y los actores involucrados en los servicios de salud y tratar de mejorar el sistema sanitario en términos de eficiencia y calidad. La compartición de la carpeta entre pacientes y su equipo de atención de salud puede mejorar la capacidad de los pacientes para el cuidado activo de su propia salud.

Es un instrumento nuevo que se ha implantado en todas las Comunidades Autónomas, aunque, salvo Galicia, ninguna ha hecho una regulación del mismo. Destaca la Orden de 19 de septiembre de 2016, de la Consejería de Sanidad de Galicia, por la que se crea y regula la carpeta personal de salud. Es preciso, pues, disponer de una normativa mínima general que fije las cautelas necesarias para proteger los datos de salud contenidos en las carpetas estableciendo las personas que podrán acceder a esos instrumentos.

VIII. INFORMACIÓN QUE HA DE FACILITARSE AL INTERESADO.

Una de las grandes novedades del RGPD es que respecto de los deberes de información al interesado por parte del responsable ahora exigibles conforme a la LOPD, amplía notablemente tales deberes de información a los interesados tanto respecto a la cantidad como a la calidad de la información que ha de facilitarse[93]. Este deber se refuerza más si cabe cuando se trata de datos especialmente protegidos como los de salud.

En efecto, apoyándose en los principios de licitud, lealtad y transparencia (considerando 39), dispone el artículo 12 RGPD que la información al interesado ha de darse en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información ha de facilitarse por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios. A su vez, los artículos 13 y 14 RGPD, en lo que aquí nos interesa, establecen que tanto en el caso de que los datos de obtengan directamente del interesado como cuando no se obtengan directamente, el responsable del tratamiento, en el momento en que los obtenga, facilitará al interesado toda la información indicada a continuación:
- la identidad y los datos de contacto del responsable y, en su caso, de su representante;
- los datos de contacto del delegado de protección de datos;
- los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

[92] SAIGÍ F., CERDÁ CALAFAT I., GUANYABENS CALVET J. y CARRAU VIDAL E. "Los registros de salud personal: el caso de la Carpeta Personal de Salud de Cataluña" en *Gaceta Sanitaria*, vol.26, núm.6, 2012, pp. 582-584.
[93] Véase *La Guía para el cumplimiento del deber de informar* conforme al RGPD elaborada por la Agencia Española de Protección de Datos, disponible en: https://www.agpd.es/portalwebAGPD/temas/.../pdf/modeloclausulainformativa.pdf

- en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional;
- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
- cuando el tratamiento esté basado en el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento;
- el derecho a presentar una reclamación ante una autoridad de control;
- cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, ha de proporcionar al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente.
- la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

Los deberes de información reseñados no son aplicables cuando y en la medida en que:
- el interesado ya disponga de la información;
- la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de investigación científica, o en la medida en que pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento.
- la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros,
- cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

IX. DEBER DE SECRETO.

1. Cuestiones generales.

1.1. Aproximación a su regulación en los códigos deontológicos y en el derecho positivo.

El secreto médico, en cuanto garantía ineludible de la confidencialidad que ha de presidir toda relación clínica para que genere confianza en el paciente, ha sido siempre un requisito o condición para el ejercicio profesional de la medicina y, como veremos, ha sido objeto de atención y regulación tanto en las normas deontológicas reguladoras del ejercicio profesional como en el derecho positivo.

El secreto ha sido una norma o regla ética de honda tradición y fuerte arraigo en la deontología médica, habiendo estado presente en todos los códigos deontológicos

médicos conocidos[94]. Entre las modernas normas deontológicas, a nivel internacional destaca el Código Internacional de Ética Médica[95] adoptado por la 3ª Asamblea General de la Asamblea Médica Mundial en Londres, en octubre de 1949 y enmendado por la 22ª Asamblea Médica Mundial en Sídney, en agosto 1968, y en la 35ª Asamblea Médica Mundial en Venecia, en octubre de 1983, que establece la siguiente norma relativa al deber del médico con sus pacientes:

> El médico debe guardar absoluto secreto de todo lo que se le haya confiado, incluso después de la muerte del paciente. El médico debe respetar la confidencialidad del paciente. Es ético revelar información confidencial cuando el paciente otorga su consentimiento o cuando existe una amenaza real e inminente de daño para el paciente u otros y esta amenaza solo puede eliminarse con la violación del secreto.

En nuestro país obligado es citar el vigente Código de Deontología Médica de 2011, que en sus artículos 27 a 30 contiene una regulación bastante completa y actual del deber de secreto y de sus excepciones.

En el marco de los convenios internacionales, el Convenio relativo a los Derechos Humanos y la Biomedicina, aprobado en Oviedo por el Comité de Ministros del Consejo de Europa el 19 de noviembre de 1996[96], establece en su artículo 10.1 el derecho a la privacidad (*privacy*) de la información en el ámbito de la salud, reafirmando el principio introducido en el artículo 8 del Convenio Europeo sobre Derechos Humanos[97], si bien, su artículo 26 permite restricciones a la privacidad por las siguientes razones:

> El ejercicio de los derechos y las disposiciones de protección contenidos en el presente Convenio no podrán ser objeto de otras restricciones que las que, previstas por la ley, constituyan medidas necesarias en una sociedad democrática para la seguridad pública, la prevención de las infracciones penales, la protección de la salud pública o la protección de los derechos y libertades de las demás personas.

Acudiendo a nuestro ordenamiento jurídico sanitario encontramos diversas normas que sientan el deber de secreto: el artículo 10 de la LGS, sanciona el secreto profesional al incluir entre los derechos básicos del ciudadano el derecho a la confidencialidad de toda información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público; el artículo 16.6 de la LBAP establece que el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto."; el artículo 5.4 de la LIB sujeta al secreto profesional a cualquier persona que ejerza funciones en relación con una actuación médico-asistencial o con una investigación biomédica; los artículos 7 y 43.2 de la LGSP se refieren específicamente a

[94] Una descripción de los Códigos Deontológicos elaborados en el periodo antiguo y en el periodo moderno y, en concreto, en España, en CASTELLANO ARROYO, M., "la deontología médica: teoría y práctica", en el libro colectivo *Derecho biomédico y bioética,* Editorial Comares, 1998, pp. 42-50.

[95] Disponible en: http://www.wma.net/es/30publications/10policies/c8/

[96] Ratificado por España mediante Instrumento de Ratificación de 23 de julio de 1999 (BOE núm. 251, de 20 de octubre de 1999).

[97] Sobre la privacidad en el ámbito sanitario conforme a nuestra Constitución véase SUÁREZ RUBIO, S., *Constitución y privacidad sanitaria,* Tirant lo Blanch, 2015.

la obligación de guardar secreto sobre los datos que faciliten los sistemas de información en el ámbito de la salud pública.

Fuera del espacio sanitario procede citar el artículo 10 de la LOPD, en cuanto establece 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 mismo.

Nuestro Código Penal tipifica en sus artículos 197 a 199 como delito, de un lado, el acceso, la difusión, la cesión, la revelación, la utilización, etc. de datos de salud (art. 197.5) sin estar autorizado o con intención de vulnerar la intimidad de otro, y de otro lado, la revelación de secretos ajenos (art. 199) distinguiendo al profesional obligado al secreto de aquellas otras personas que por razón de su oficio o relación laboral tengan conocimiento de secretos ajenos, y castigando con mayor pena a los profesionales. Respecto de estos, la STS de 4 de abril de 2001 -RJ/2001/2016- señala que "*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 reglamentada. Y es que cuando el art. 199.2 alude a profesional se está refiriendo a una profesión que exige un título académico u oficial, que exige normalmente una colegiación para su ejercicio y que tiene unas normas deontológicas reglamentadas*"[98]. El artículo 201 los tipifica como delitos semiprivados.

Así pues, el secreto es un deber inexcusable tanto del profesional sanitario como de las personas que acceden a datos de salud[99] y genéticos[100] o los tratan. Empero, tanto la legislación sanitaria como la de enjuiciamiento criminal establecen límites o excepciones al deber de secreto, exonerando al profesional de ese deber en determinadas circunstancias y obligándole en otras a denunciar o declarar los datos que conoce. De ahí que la doctrina ha acuñado el concepto de "secreto médico relativo" asumiendo el hecho de que la pretensión de otorgar al secreto un carácter absoluto haciendo prevalecer siempre la conveniencia individual o privada puede implicar en ocasiones un perjuicio para los intereses generales. Como señalan CASTELLANO y GISBERT[101], con la aceptación de la relatividad del secreto médico y el arrinconamiento del secreto médico absoluto lo que se pretende es buscar el equilibrio

---

[98] Al respecto, véase la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

[99] El artículo 4 del RGPD define los datos de salud como "*datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud*."

[100] El artículo 4 del RGPD define los datos genéticos como "*datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.*"

[101] CASTELLANO, M, GISBERT, JA. "El secreto médico. Historia clínica. Confidencialidad y otros problemas médico-legales de la documentación clínica", en el libro colectivo *Medicina legal y toxicología*. 6ª ed., Ed. Masson, S.A; 2004, pp. 93-108.

entre el derecho individual que supone la protección de la intimidad de la persona y determinados derechos colectivos como pueden ser la salud pública, la administración de justicia, etc. Por ello, afirman, en medicina el secreto es relativo y se entiende como la obligatoriedad de su guarda por parte del médico respecto al estado de salud y confidencias del paciente, pero siempre que no se perjudique por ello a los demás, a los intereses sociales, o a los intereses generales.

Las normas españolas antes citadas no han trazado un régimen jurídico preciso del secreto y de sus excepciones que dé seguridad jurídica a los profesionales sanitarios. Los artículos 20.1.d) y 24.2 CE disponen que una Ley regule el secreto profesional, pero todavía no se ha aprobado dicha ley. Entonces, explorando nuestro ordenamiento jurídico nos encontramos con un deber de secreto plagado de excepciones explicitadas en diversas normas de diferente rango e insuficientemente perfiladas, lo que obliga frecuentemente al profesional sanitario a tomar decisiones sin suficiente amparo jurídico-normativo y también le sitúa ante dilemas difíciles de resolver tanto desde el punto de vista jurídico como ético. A esta dificultad ha de añadirse el hecho de que la mayoría de las modernas profesiones sanitarias y de las personas que por su oficio o relación laboral acceden a datos de salud y los tratan, carecen de cultura de secreto y confidencialidad y de códigos éticos al respecto, como la tienen los médicos[102].

Para finalizar este apartado, señalar que el anteproyecto de Ley Orgánica de Protección de Datos Personales que ha elaborado el Ministerio de Justicia y ha hecho público el 30 de junio de 2017, que sustituirá a la vigente LOPD, respecto al secreto profesional se limita a establecer lo siguiente:

> Artículo 6. Deber de confidencialidad.
> 1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de éste estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1 f) del Reglamento (UE) 2016/679.
> 2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.
> 3. Las obligaciones establecidas en los apartados anteriores se mantendrán con carácter indefinido, aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Este artículo sustituirá al artículo 10, transcrito supra, de la vigente LOPD. Comprobamos, por tanto, que se sigue postergando la regulación del secreto profesional.

1.2. Evolución del deber de secreto.

Desde la entronización del Juramento Hipocrático hasta mediados del siglo XX el secreto médico se sitúa y desarrolla en el ámbito de la ética médica, sin que apenas sea objeto de atención por parte del derecho positivo. Es bien entrados en el siglo XX

[102] Realmente, el régimen más completo y acabado del secreto médico y de sus excepciones se encuentra descrito en los artículos 27 al 30 del vigente Código de Deontología Médica de 2011.

cuando el secreto médico se remodela paulatinamente al agregar nuevas dimensiones en razón de dos elementos confluyentes: de un lado, la incorporación por la Constitución de 1978 a nuestro acervo normativo de los derechos fundamentales a la intimidad[103] y a la protección de los datos personales, lo que le confirió una dimensión jurídica antaño prácticamente inexistente pues el secreto, de ser solo un deber ético del médico en una concepción paternalista del mismo, pasó a ser también un derecho del paciente a la salvaguardia de su intimidad frente a terceros, y de otro, el cambio habido en la relación clínica ya que la tradicional relación médico-paciente sin interferencias ha evolucionado hasta llegar a la práctica de la medicina en equipo en un contexto de alta tecnología, lo que, a su vez, ha provocado que el secreto trascienda a la figura del médico y se extienda a la generalidad de las profesiones sanitarias y a otras personas implicadas directa o indirectamente en las actividades sanitario-asistenciales, dando lugar a lo que se ha venido en denominar secreto médico compartido y secreto médico derivado. En suma, el secreto ya no es cuestión que ataña exclusivamente al binomio médico-paciente sino que implica a un equipo asistencial con el paciente. Esta evolución impulsó a María CASADO[104] a preguntarse si es la misma confidencialidad la que apelaba al deber de guardar el secreto profesional del tradicional médico de cabecera que la que ahora resulta amenazada con la informatización de las historias clínicas y su manejo. Obviamente, es un contexto muy diferente y preservar esa confidencialidad exige hoy unos mecanismos técnicos y jurídicos antes innecesarios. Entre los mecanismos técnicos para preservar el secreto cabe citar en el ámbito de la historia clínica electrónica las restricciones de acceso, los códigos de acceso, los registros de acceso y los módulos de especial custodia, y en el ámbito de la investigación científica la anonimización y la seudonimización. Entre los jurídicos procede citar la paulatina incorporación a leyes y reglamentos de la definición del contenido y alcance del deber de secreto de profesionales y personas que acceden y maneja datos de salud, así como la tipificación de infracciones administrativas y penales y de las correspondientes sanciones por el acceso y uso indebido de datos de salud.

A partir de mediados del siglo XX, el secreto médico, además de en el ámbito asistencial, también tiene una presencia muy importante en las actividades de salud pública y en la epidemiológica en cuanto estas disciplinas trascienden la clásica función de vigilancia de las enfermedades transmisibles y se extienden al estudio de la frecuencia y distribución de los fenómenos relacionados con la salud y sus determinantes en poblaciones específicas, para lo que manejan ingentes cantidades de datos de salud provenientes de diferentes fuentes y trabajan frecuentemente con datos de salud personalizados, razón por la que el RGPD (art. 9.2.i) y la LGSP (art.43.2) sujetan a los investigadores epidemiólogos al secreto profesional.

Situados en pleno siglo XXI, no es exagerado afirmar que el deber de secreto nuevamente está en crisis por causa del reciente crecimiento exponencial del

[103] Auto del TC 600/1989, de 11 de diciembre, que se transcribe más adelante.

[104] CASADO M. "Los derechos humanos como marco para el bioderecho y la bioética" en el libro colectivo ROMEO CASABONA, C. (director) *Derecho biomédico y bioética,* Editorial Comares, 1998, p. 175.

tratamiento automatizado de datos de salud en cantidades ingentes (grandes bancos informatizados de datos clínicos), lo que ha dado lugar al fenómeno denominado *big-data*, y también por causa de la explosión de la sanidad electrónica. El deber de secreto se desenvuelve ahora en la era de la electrónica (telemedicina, telesalud, etc.)[105] y del *big-data,* y aunque facilitan la asistencia al enfermo también ponen en serio riesgo su derecho a la intimidad.

1.3. Concepto de secreto y alcance del deber.

Propuesta de regulación:

1. Por secreto ha de entenderse el deber de reserva o sigilo que grava a cualquier profesional o persona que realice actividades en el ámbito de la salud, en relación con los datos personales que llegue a conocer directamente de la persona titular de los mismos, por la realización de determinadas pruebas o por otras vías, o que tenga acceso a ellos con ocasión de su tratamiento conforme a la definición de tratamiento que hace el artículo 4.2) del Reglamento (UE) 2016/679, de 27 de abril de 2016.

2. El deber de secreto comprende lo concerniente a la esfera privada de la persona, que es solo conocido por su titular o por quién él determine. Engloba aquellos extremos afectantes a la intimidad que tengan cierta relevancia jurídica en cuanto su revelación lesione la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, ámbito necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de vida humana [106].

3. La comunicación o cesión de datos de salud anonimizados irreversiblemente no afecta al deber de secreto.

Comentario exegético:

De entrada, conviene hacer alguna precisión en cuanto a la terminología utilizada por la normativa que regula o hace alusión al deber de secreto. El artículo 6.2 del anteproyecto de la nueva LOPD y el artículo 9.2 del RGPD hablan de "secreto profesional", y ya sabemos que nuestro Código Penal diferencia entre el profesional obligado al secreto y las personas que por razón de su oficio o relación laboral tengan conocimiento de secretos de otras personas, castigando con mayor pena al profesional. A su vez, el artículo 9.3 del RGPD diferencia al "profesional sujeto a la obligación de secreto profesional" de "cualquier otra persona sujeta también a la obligación de secreto". Por su parte, los artículos 16.6 de la LBAP, 51.1 de la LIB y 43.2 de la LGSP hablan de "deber de secreto", sin adjetivarlo de "profesional", esto es, como un deber genérico aplicable a todas las personas que acceden, conocen y tratan datos de salud. Por tanto, cuando en este trabajo se habla de "deber de secreto" se hace con el propósito de que

[105] Sobre estas cuestiones véase al reciente libro colectivo PÉREZ GÁLVEZ, J. F. (director) *Salud Electrónica. Perspectivas y Realidad*, Tirant lo Blanch, 2017.
[106] Conforme a la doctrina que sienta la STS 4 abril 2001 -RJ/2001/2016-.

esta expresión acoja tanto a las profesiones sanitarias tituladas reguladas y colegiadas como al resto de personas que ejercen oficios y labores en el ámbito de la salud y acceden y tratan datos de salud. En definitiva, con el alcance subjetivo que le dan las citadas leyes sanitarias.

Según nuestro Tribunal Constitucional[107], "*el secreto profesional, en cuanto justifica, por razón de una actividad, la sustracción al conocimiento ajeno de datos o informaciones obtenidas que conciernen a la vida privada de las personas, está estrechamente relacionado con el derecho a la intimidad que el art. 18.1 de la Constitución garantiza, en su doble dimensión personal y familiar, como objeto de un derecho fundamental. 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*." Atendiendo a esta doctrina, se ha dicho que la conexión entre el derecho a la intimidad y el secreto profesional es "la necesidad" de abrir la intimidad a un tercero en la confianza de que el secreto no va a ser revelado, creándose así un deber de fidelidad[108]. Por su parte, el Tribunal Supremo[109], con apoyo en la citada doctrina del TC, desarrolla el concepto de intimidad en su variante de situación médica o sanitaria entendiendo que "*ha de referirse a todo aquel conjunto de cualidades inmanentes a la propia persona afectada que están tan estrechamente unidas a su propia naturaleza corporal que no solo se incardinan desde un punto de vista somático, a todo lo que concierne a su propia fisiología, tanto en su génesis constitutiva como en su porte exterior, sino que abarca su acervo actuatorio tendente a indispensables actos de pervivencia o desarrollo con un sello personalísimo cuya indemnidad ha de estar tutelada frente a cualquier injerencia extraña"*. En suma, el secreto se sitúa en el marco del derecho fundamental a la intimidad.

La Agencia Española de Protección de Datos, en su resolución R/01326/2008, de 2 de octubre, se refiere al deber de secreto en esos términos: "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 CE. En efecto, este precepto contiene un instituto de garantía de los derechos de los ciudadanos que, además, 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. Este 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 que

[107] Auto del Tribunal Constitucional 600/1989, de 11 de diciembre.
[108] SUÁREZ RUBIO, S. *Constitución y privacidad sanitaria,* Tirant lo Blanch, 2015, p. 157.
[109] Sentencia de la Sala Primera del Tribunal Supremo de 4 de mayo de 2001 -RJ/2001/2043-.

impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida."

Conforme al reseñado marco jurisprudencial, GARCÍA SANZ[110] enmarca el secreto médico en el "derecho del paciente a salvaguardar su intimidad frente a terceros, e incluiría toda información, conocida por el paciente y otra u otras personas pertenecientes a un círculo reducido, que la persona afectada no desea sea revelada o divulgada a terceros". Por su parte, GÓMEZ RIVERO[111] ha identificado los siguientes fundamentos garantistas para tutelar el secreto en el ámbito sanitario: el primero y más importante, la protección de la intimidad de las personas titulares de los datos de salud. Junto a este fundamento primario identifica las siguientes garantías: a) atendiendo al clima de confianza necesario para que cualquier persona demande servicios sanitario-asistenciales, preservar una suerte de apriorística garantía de "fidelidad profesional"; b) atendiendo a los intereses del colectivo de profesionales sanitarios: en primer lugar, garantía de que el profesional pueda obtener toda la información que necesite para el tratamiento que se le confía; en segundo lugar, la tranquilidad y seguridad que la institución del secreto reporta para el profesional a la hora de solicitar datos; y en tercer lugar, la garantía de que no puede ser obligado por el propio paciente a revelar datos relativos a terceras personas.

Con la transcripción de estos pronunciamientos sobre el secreto se pretende dejar bien sentado el hondo fundamento jurídico y ético de este deber anclado directamente en el derecho fundamental a la intimidad protegido por el artículo 18.1 CE. Ahora bien, no es factible intentar de forma apriorística acotar el tipo o ámbito de los datos comprendidos por el secreto en función de su trascendencia para preservar de una forma efectiva la intimidad de la persona. Puede afirmarse, no obstante, que como regla general se comprenden en el secreto sanitario todos los datos -físicos, psicológicos, de salud- que se obtengan de la relación clínica entablada con el paciente[112]. En cualquier

---

[110] GARCÍA SANZ, J., "El secreto profesional en el ámbito sanitario" en *Estudios Jurídico-Penales sobre Genética y Biomedicina, Libro Homenaje al Prof. Dr. D. Ferrando Mantovan*i, Dykinson, 2005, p. 463.

[111] Cit., pp. 1500-1502.

[112] La Orden SSI/81/2017, de 19 de enero, por la que se publica el Acuerdo de la Comisión de Recursos Humanos del Sistema Nacional de Salud, por el que se aprueba el protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en ciencias de la salud, en su apartado 8.2 fija el siguiente ámbito de los datos comprendidos en el deber de secreto: *Tanto residentes como alumnos están sometidos al deber de confidencialidad/ secreto, no solo durante la estancia en el Centro sanitario en el que se esté formando sino también una vez concluida la misma, sin que dicho deber se extinga por la defunción del paciente. El deber de confidencialidad afecta no solo a «datos íntimos» (incluidos los psicológicos relativos a ideas, valores, creencia, vivencias personales…) sino también a datos biográficos del paciente y de su entorno (sean íntimos o no) cuyo conocimiento por terceros pueda afectar a los derechos de la persona objeto de tratamiento. El deber de confidencialidad/secreto no solo se refiere a los datos contenidos en la historia clínica del paciente sino también a los que se ha tenido acceso mediante comunicación verbal, grabaciones, vídeos, así como a los contenidos en cualquier tipo de archivo informático, electrónico, telemático o registro público o privado, incluidos los referidos al grado de discapacidad e información genética. El deber de secreto se entiende sin perjuicio de los supuestos legales en los que su mantenimiento implique riesgo para la vida del afectado o de terceros o perjuicio para la Salud Pública, en cuyo caso se pondrá en conocimiento de los responsables asistenciales del correspondiente servicio/unidad asistencial para que se actúe en consecuencia.*

caso, el deber de secreto no se extiende y no debe extenderse a aquellos hechos o circunstancias que no tengan la consideración de íntimos y que, por lo tanto, su revelación no sea susceptible de lesionar la intimidad del paciente. Así, por ejemplo, no quedarían amparados por el secreto médico los datos relativos a si hubo o no información suficiente por parte de los médicos a efectos de obtener el consentimiento informado del paciente, pues tales datos carecen de relevancia jurídica a efectos de preservar la intimidad, la privacidad del sujeto.

En cuanto al alcance de este deber, importa resaltar que no es un valor absoluto pues cederá cuando se enfrenta a otros bienes de igual o superior valor siempre que haya previsiones legales o deontológicas exonerando de la observancia de dicho deber. Y, en efecto, encontramos previsiones en este sentido en todos los ordenamientos jurídicos habilitando u obligando a los profesionales sanitarios o comunicar o ceder a terceros los datos de salud que conoce a fin de preservar bienes de interés público como la salud pública o individuales como la vida, la salud o la integridad física de las personas. El artículo 3 de la LOPD define la cesión o comunicación de datos como "toda revelación de datos realizada a una persona distinta del interesado." La revelación del secreto sin el consentimiento expreso del interesado -si hay consentimiento no hay violación del secreto- en los supuestos en que es legítima, implica la cesión o comunicación de datos de salud a un tercero: a una persona física distinta al interesado, a un profesional sanitario, a un órgano administrativo, a un órgano judicial, a autoridades sanitarias, a autoridades de control de tratamiento de datos, etc. Y la cesión o comunicación de datos es tratamiento de datos conforme a la definición de "tratamiento" que hace el artículo 4.2 del RGPD. No obstante, conviene diferenciar entre cesión de datos (cedente y cesionario), que se desenvuelve en el marco de la legislación de protección de datos (infracción administrativa -art. 44.3.k- LOPDP), y la violación del deber de secreto profesional (actuación de una persona física) considerada como delito (infracción penal).

1.4. Sujetos implicados.

Propuesta de regulación:

1. Queda sujeta al deber de secreto cualquier persona[113] *que realice o participe en actuaciones asistenciales o preventivas sobre pacientes, o que realice funciones de administración, gestión, planificación o inspección, así como la que realice estudios o investigaciones en el ámbito de la salud pública, en relación con los datos que llegue a conocer directamente de la persona titular de los mismos o que tenga acceso a ellos a través de la consulta de la historia clínica, o por cesión o comunicación de otras personas o entidades. Este deber persistirá aun una vez haya cesado en la actividad que le haya habilitado a acceder y tratar los datos.*

[113] El artículo 9.3 RGPD extiende el secreto a los profesionales y a cualquier otra persona sujeta a la obligación de secreto de acuerdo con el RGPD y el derecho de los Estados miembros. La LBAP habla de personas sujetas a secreto, no de profesionales. La LIB también habla de personas sujetas a secreto.

Este deber también se extiende al responsable del tratamiento[114]*, a quienes intervengan en cualquier fase del tratamiento de los datos*[115]*, y a los delegados de protección de datos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*[116]*.*

2. La confidencialidad de los datos clínicos impone al profesional sanitario, además de su deber de sigilo, instruir en este deber a quienes trabajan junto a él o a aquellos de cuya formación es responsable.

En el inicio de una investigación epidemiológica los profesionales y personal implicados deberán ser informados suficientemente del deber de secreto desde el punto de vista jurídico y ético y suscribir un documento que les comprometa al secreto profesional.

Comentario exegético:

En primer lugar, recordemos que la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias, habla de "profesiones sanitarias tituladas" determinando taxativamente cuáles son (artículo 2) y de profesionales del área sanitaria de formación profesional (artículo 3) enumerando también estas profesiones. Por su parte, el RGPD y la LBAP, en relación con la protección de datos de salud hablan de "profesionales sanitarios" y de "personal sanitario" en una acepción amplia con la que se quiere englobar todas aquellas personas que desarrollan su labor profesional en centros y servicios sanitarios, pero que su titulación o formación profesional no encaja en las enumeraciones que hace la citada Ley de Ordenación de las Profesiones Sanitarias. Y es que en el ámbito sanitario tienen acceso a datos de salud, además de las profesiones sanitarias tituladas, profesionales del área sanitaria de formación profesional, administrativos, psicólogos, gestores, estudiantes, técnicos informáticos, trabajadores sociales, etc. La epidemiología en sus variantes biomédica y social es una disciplina multiprofesional[117] que acoge a médicos, enfermeros, biólogos, farmacéuticos,

[114] Conforme al artículo 4 del RGPD: *«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*. Y conforme al artículo 3 de la LOPD: *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.*

[115] Según el ATC de 11 de diciembre de 1989 "*El deber de secreto en el tratamiento de datos personales, tiene la misma fundamentación jurídica, pero se refiere al ámbito estricto del tratamiento de los datos personales, para que el responsable del fichero y, cualquier persona que intervenga en el tratamiento, esté obligado al mantener la confidencialidad de los datos personales* ".

[116] Este texto pretende ser un compendio de los siguientes preceptos legales: artículos 2.7 y 16.6 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente; artículos 5.4 y 51 de la Ley 14/2007, de 3 de julio, de Investigación Biomédica; y 10 de la LOPD: *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*.

[117] Véase LÓPEZ, M.ª J, y CONTINENTE, X., "Ser joven y dedicarse a la epidemiología: ¿sinergia de factores de riesgo?, en *Gaceta Sanitaria,* 2014, 28(1), pp.1-3.

estadísticos, psicólogos, sociólogos, antropólogos, trabajadores sociales, etc. El RGPD, la LBAP y la LOPD sujetan a todos ellos al deber de secreto respecto de los datos de salud personalizados que conocen.

Sin embargo, no está convenientemente regulado para este amplio colectivo un equivalente al secreto profesional que rige la relación médico-paciente. Es más, la mayoría de estas profesiones carecen de una cultura del secreto y la confidencialidad como la que tienen las profesiones sanitarias tituladas generada por sus tradicionales normas deontológicas. Es frecuente la invasión de la intimidad del paciente por los profesionales y el personal sanitario no por razones más o menos justificadas de necesidades sanitarias técnicas o científicas, sino simplemente por ignorancia de este deber o por mera curiosidad o simple cotilleo. Ello es debido a la falta de formación y concienciación del personal sanitario en este deber de preservar la intimidad del paciente.

En suma, todo el personal sanitario, tanto profesionales como en particular aquellos que no pertenezcan a una profesión sanitaria titulada, en cuanto manejan datos que afectan a la intimidad y privacidad de las personas, deben ser informados, entrenados y educados en la confidencialidad y en el deber de secreto, y deben sumir expresamente compromisos de confidencialidad. Es, por tanto, necesario la implementación de programas de información y educación y promuevan que estas personas, desde su incorporación al puesto de trabajo, la adquieran competencias y hábitos de manera que el respeto a la intimidad de las personas esté interiorizado en su quehacer diario[118]. Son medidas de seguridad, y la seguridad es uno de los pilares del RGPD.

Finalmente, hay que tener presente que el RGPD establece que el responsable y el encargado del tratamiento de datos pueden ser personas físicas y jurídicas (artículo 4, apartados 7 y 8), y en el artículo 5 los somete al deber de secreto profesional. Por tanto, el deber de secreto se extiende no solo a las personas físicas sino también a las jurídicas[119].

2. Excepciones al deber de secreto: secreto compartido.

[118] Se trata de prevenir y evitar casos como el ocurrido en el Servicio Navarro de Salud-Osasunbidea, que fue condenado (Sentencia del Juzgado de lo Contencioso-Administrativo, de 25 de mayo de 2011 -RJCA/2011/835- confirmada por la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Navarra, de 8 de febrero de 2012 -RJCA/2012/143-) al abono de una importante indemnización a los familiares de una joven ingresada en un centro hospitalario que falleció, por la vulneración del derecho a la intimidad y a la protección de sus datos, al haberse acreditado que su historia clínica electrónica había sido objeto de 2.825 accesos por 417 usuarios diferentes adscritos a 55 servicios médicos distintos pertenecientes a 4 hospitales, cuando habían sido únicamente 4 servicios de un mismo hospital los que habían intervenido en la asistencia a la paciente. Otro caso más reciente con condena: STS de 23 de septiembre de 2015, nº 532/2015.

[119] La vigente LOPD se expresa en similares términos. Véanse la Resolución de 18 de enero de 2013 de la Agencia Española de Protección de Datos -JUR/2013/118910-, por la que se impone una sanción a una entidad financiara por infracción del artículo 10 de la LOPD, y la Resolución de 30 de mayo de 2007, R/00345/2007, en la que la Agencia consideró que la información efectuada por el Ayuntamiento de Miranda de Ebro a los medios de comunicación de los hechos que motivaron una sanción disciplinaria y las razones que impidieron su ejecución, constituyen una infracción del deber de confidencialidad que exige el artículo 10 de la LOPD

2.1. Introito.

El artículo 16 de la LBAP permite el tratamiento de datos de salud sin consentimiento del interesado con fines de medicina preventiva, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario, gestión de los centros y servicios de asistencia sanitaria, por razones de salud pública y epidemiológicas, de investigación y docencia, evaluación y acreditación de centros sanitarios, planificación sanitaria, y para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria. En todos estos casos se ceden o comunican datos de salud a otros profesionales sanitarios o a autoridades u órganos administrativos con quebranto del deber de secreto, y los que los reciben, a su vez, tratan esos datos. Pues bien, el citado artículo 16 sujeta a estas personas que reciben los datos al deber de secreto. El anteproyecto de nueva LOPD, como sabemos, remite el tema a una ley específica que sustituirá a este artículo. Por su parte, el RGPD (artículo 9.2, apartado h), y 3) implícitamente exime del deber de secreto a los profesionales que ceden los datos por las razones antedichas y, a la par, sujeta expresamente a los profesionales y órganos administrativos que reciben y tratan esos datos al deber de secreto profesional. Estamos, pues, de facto, ante confidentes necesarios por exigencia normativa y ante un secreto compartido.

En este sentido, comentando el artículo 199 del Código Penal, GARCÍA ALBERO[120] hace alguna referencia al derecho comparado relatando que "*En la legislación comparada, el par. 203 StGB alemán*[121]*, prevé un exhaustivo listado relativo al personal médico sanitario sometido a la exigencia penal de sigilo, en el que se menciona a los médicos, dentistas, farmacéuticos, psicólogos profesionales y a cualesquiera otras personas cuya ocupación -reglada por el Estado- se relacione con la salud de las personas. Además, el legislador alemán ha extendido la obligación de sigilo a los integrantes de empresas privadas de seguros relacionadas con los datos sanitarios de las personas (seguros de vida, de accidentes o de enfermedad) y a las organizaciones médicas privadas (par. 203 StGB Abs. 3); en igual sentido establece la equiparación, a los efectos del deber de sigilo, a quienes actúan profesionalmente como ayudantes y a las personas encargadas de la preparación de la actividad profesional. También el Codice Penale italiano (art. 622) permite, a través del sistema de cláusula genérica, extender la obligación de secreto profesional al personal sanitario auxiliar.*" Nuestro Código Penal no sigue esta técnica.

A juicio de GARCÍA ALBERO, la solución postulable debe ser la de proyectar la obligación de secreto profesional «ex» artículo 199.2 del Código Penal a todas aquellas personas erigidas en «confidentes necesarios», sometidos a una obligación de reserva reglada por el Estado. Así, la doctrina que ha estudiado el deber de secreto en el ámbito

[120] *Comentarios al Código Penal,* Tomo II, Editorial Aranzadi, 2008.
[121] Código Penal Alemán.

sanitario en el marco de nuestro ordenamiento jurídico[122], se ha ocupado de esta realidad alumbrando las siguientes variantes del secreto médico:

- Secreto médico compartido: obliga a toda persona que, por su actividad profesional, está implicada directamente en la atención sanitaria del paciente junto al médico responsable (otros médicos especialistas del equipo, enfermeras, matronas, auxiliares de clínica, trabajadores sociales, etc.).

- Secreto médico derivado: la complejidad actual de los centros y servicios asistenciales exige a personas, que no participan directamente en la atención sanitaria del enfermo, a conocer datos confidenciales de los pacientes atendidos en razón de su necesaria labor para el correcto funcionamiento del centro (administrativos, técnicos, gestores, etc.). Obviamente, quedan obligadas al secreto.

Como vemos, estas construcciones doctrinales, tanto la penal como la sanitaria, se han centrado exclusivamente en el ámbito de la asistencia sanitaria, ignorando otros ámbitos no asistenciales donde también se produce una comunicación o cesión de datos de salud personalizados entre profesionales sanitarios, obligados todos ellos por el deber de secreto[123]. Y en efecto, también es viable acudir a la institución del secreto médico compartido para enmarcar las comunicaciones de datos a facultativos ajenos al proceso asistencial de paciente por razones de protección de la salud pública, de medicina preventiva y para lograr buenos niveles de calidad asistencial, por lo que seguidamente razonamos.

Entre las excepciones establecidas normativamente al deber de secreto, que encajan en la noción de secreto compartido, se sitúan los supuestos en los que, como confidentes necesarios, el médico debe comunicar a una autoridad sanitaria o a un órgano administrativo público sanitario, cuyos titulares son también médicos, determinados datos de salud que ha conocido con ocasión de su ejercicio profesional, por lo que técnicamente existe o se produce una revelación del secreto. Ahora bien, hay una diferencia sustancial que no se da en el resto de los supuestos legalmente establecidos en los que se excepciona el deber de secreto, y es que la comunicación de los datos se produce exclusivamente entre médicos o profesionales sanitarios y en el ámbito de la actividad sanitaria pública, mientras que en el resto de los casos se produce entre el

[122] Véase, DE MIGUEL, N., *Secreto médico, confidencialidad e información sanitaria,* Marcial Pons, 2002, pp. 308-311; TRONCOSO REIGADA, A., La protección de datos sanitarios: la confidencialidad de la historia clínica" en el libro *La protección de datos personales para Servicios Sanitarios Públicos,* Thomson-Civitas, 2008, p. 85; FERNÁNDEZ PANTOJA, P., "El delito de revelación y divulgación de secretos en el ámbito sanitario", en el libro colectivo, *Estudios jurídicos sobre responsabilidad penal, civil y administrativa del médico y otros agentes sanitarios,* Edit. Dykinson, 2010, p. 294; DE LORENZO, R., *El secreto médico derivado,* en Redacción Médica de 11 de febrero de 2013, disponible en: https://www.redaccionmedica.com/opinion/el-secreto-mdico-derivado-4970

[123] Llama la atención comprobar que no existe en nuestro país ninguna literatura científica que analice el deber de secreto y sus excepciones desde la perspectiva de las actuaciones de salud pública. Repasados los abundantes trabajos jurídicos que analizan el deber de secreto y sus excepciones se comprueba que se centran exclusivamente en el ámbito de la asistencia sanitaria e ignoran sistemáticamente el de la salud pública. Ello posiblemente es debido a la que la salud pública siempre ha sido y sigue siendo la cenicienta del sistema sanitario.

profesional sanitario y terceras personas totalmente ajenas al sector sanitario: personas físicas particulares, jueces, funcionarios judiciales que intervinieron en la tramitación de un asunto, letrados que participaron en el proceso en defensa y representación de los litigantes, defensores del pueblo, empresarios, etc. Además, la comunicación de datos en estos casos, esto es importante resaltarlo, se produce fuera del circuito estricto de la actividad sanitaria pública.

Así pues, hay dos notas esenciales que enmarcan el deber de secreto compartido: la comunicación es entre profesionales que desempeñan su labor en el ámbito sanitario, que actúan en calidad de confidentes necesarios, y lo es en el marco de la actividad sanitaria de la Administración pública. Como acertadamente se ha apuntado[124] no se trata de revelar un secreto en sentido amplio, sino de transmitir una información médica a otros médicos y/o autoridades que actuarán también en beneficio del paciente y de la colectividad, por lo que quedan igualmente obligados a la salvaguardia y protección del secreto. En el resto de los casos no media una actividad sanitaria pública de carácter preventivo, sino el motivo de la comunicación de los datos es resolver un conflicto judicial o tratar de evitar el riesgo grave e inminente que amenaza a una o varias personas físicas, ámbitos estos donde es difícilmente predicable la institución del deber de secreto compartido. No hay, pues, el nivel de confidencia que existe entre los profesionales sanitarios en el ejercicio de sus respectivas funciones. Téngase presente que en el ámbito judicial son públicas las actuaciones judiciales (artículo 120.1 CE y artículo 232 de la Ley Orgánica del Poder Judicial) y, normalmente, se practican en audiencia pública las diligencias de prueba y las vistas de los pleitos (excepcionalmente, por razones de orden público y de protección de los derechos y libertades, los jueces y tribunales, mediante resolución motivada, pueden limitar el ámbito de la publicidad y acordar el carácter secreto de todas o parte de las actuaciones), por lo que generalmente es inevitable la propagación de los datos privados a cualquiera que hubiera asistido a las actuaciones desplegadas en un pleito. De otro lado, resulta poco operativo intentar someter al deber de secreto compartido a personas físicas particulares a las que se ha comunicado determinados datos de un tercero a fin de evitarles un riesgo grave. No hay secreto compartido, no hay confidencialidad, sino lo que reamente se produce es la divulgación de un secreto; ocurre lo que se puede denominar como secreto divulgado.

En suma, es sostenible que el secreto compartido, estudiado desde una óptica técnico-jurídica, no implica o conlleva una ruptura del deber de secreto, cosa que sí ocurre respecto del secreto divulgado. En línea con esta posición cabe citar el artículo 14.5 del RGPD, en el que, respecto de los datos que no se han obtenido del interesado, se exime al responsable del deber de informarle cuando esos datos deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la UE o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria. El legislador europeo implícitamente está reconociendo que no hay revelación del secreto, sino mera cesión o comunicación de datos entre confidentes necesarios, lo que hace baladí informar al interesado.

[124] VALERIO, C., voz "SIDA" en ROMEO CASABONA (director) *Enciclopedia de Bioderecho y Bioética*, Tomo II, edit. Comares, 20111, p. 1531.

Los ámbitos que han sido objeto de regulación en los que la norma claramente ha perfilado un deber de secreto compartido son los siguientes: a) declaración de enfermedades transmisibles; b) vigilancia en salud pública; c) comunicación de datos de salud entre Administraciones sanitarias para el ejercicio de competencias iguales o sobre materias iguales y para fines de investigación científica; d) comunicaciones a registros nominales de vacunación y farmacovigilancia; e) asistencia sanitaria pública y privada.

Pueden identificarse otros ámbitos de control en los que sería conveniente posibilitar normativamente la cesión o comunicación de datos de salud sujetándola a las reglas del secreto compartido. Así, por ejemplo, la Declaración de 8 de julio de 2017 de la Comisión Central de Deontología del Consejo General de Colegios Médicos, sobre el secreto médico, incluye los certificados de aptitud (conducción, uso de armas) entre los procedimientos de control que merecen una especial consideración a efectos de transmitir información con la consiguiente ruptura del secreto médico, respecto de los que propone una conexión entre los médicos de atención primaria y hospitalaria, públicos y privados, y los centros homologados, mediante la cual los profesionales podrían advertir que las condiciones de salud de la persona han cambiado, para que esta fuera requerida en breve espacio de tiempo a un nuevo examen por el centro homologado para evaluar, a la luz de la nueva situación, la confirmación o la denegación de la aptitud para la actividad concreta para la que fue concedido el certificado de aptitud. La Declaración concluye recomendando que se establezca un marco normativo que facilite canales de comunicación estables entre la medicina asistencial, pública y privada, la medicina del trabajo y los centros de acreditación de capacidades psicofísicas, que debe entenderse no como una ruptura de la confidencialidad, sino como una ampliación del círculo de confidentes necesarios para una correcta asistencia integral al paciente y la protección de la sociedad (nos abstenemos en este trabajo de intentar una propuesta de regulación puesto que excedería ampliamente de su ámbito propio).

Por lo demás, sería conveniente estudiar la posibilidad de incorporar a la futura ley reguladora del secreto profesional sanitario un artículo que defina el secreto compartido como una variable del secreto profesional y que acote los sujetos que lo practican en términos similares a la siguiente propuesta:

Quedan sujetos al deber de secreto compartido, como confidentes necesarios, los profesionales sanitarios y no sanitarios en relación con los datos de salud que, por comunicación de otros profesionales o por acceso directo legítimo a los historiales clínicos cedidos por las administraciones públicas y entidades privadas, lleguen a conocer y a tratar por necesidad del ejercicio de su función o labor profesional en el ámbito de la asistencia sanitaria, la salud pública y la investigación epidemiológica.

2.2. Declaración de enfermedades transmisibles.[125]

Propuesta de regulación:

1. La declaración obligatoria a los órganos competentes de la Administración sanitaria autonómica de las enfermedades transmisibles relacionadas en la normativa correspondiente, se refiere a los casos nuevos de estas enfermedades aparecidos durante la semana en curso y bajo sospecha clínica, y corresponde realizarla a los médicos en ejercicio, tanto del sector público como privado.

2. La declaración de los casos será nominal, debiendo aportar datos epidemiológicos como la edad, sexo, lugar de residencia, fecha de inicio de síntomas, antecedentes de vacunación en caso de enfermedad susceptible de inmunización, en cuanto son fundamentales para la caracterización del comportamiento de las enfermedades en la población.

Se establecerán protocolos para homogeneizar el contenido, la forma de declaración según la definición de los casos y el procedimiento automatizado de notificación desde la historia clínica electrónica.

3. Los responsables de los registros disociarán los datos personales de los de salud mediante procedimientos de seudonimización.

4. El acceso a los datos comunicados habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional.

Comentario exegético:

Las medidas utilizadas al servicio de la prevención de las enfermedades transmisibles son variadas. Una de ellas, utilizada desde antaño, es la declaración obligatoria a la Administración sanitaria de tales enfermedades por cuanto ha demostrado ser unos de los instrumentos más útiles en la lucha contra las enfermedades infecto-contagiosas. De ahí que, excepcionando el deber de secreto, normativamente se obligue a los médicos a

[125] Sobre el control de enfermedades transmisibles cabe citar la siguiente legislación:
- Ley Orgánica 3/86, de 14 de abril, de Medidas Especiales en Materia de Salud Pública:
Artículo 3: Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que están o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible.
- Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica:
Artículo 9. Las enfermedades objeto de declaración obligatoria se relacionan en el anexo I de este Real Decreto. La declaración obligatoria se refiere a los casos nuevos de estas enfermedades aparecidos durante la semana en curso y bajo sospecha clínica, y corresponde realizarla a los médicos en ejercicio, tanto del sector público como privado.
- Decisión n.º 1082/2013/CE del Parlamento Europeo y del Consejo de 22 de octubre de 2013 sobre las amenazas transfronterizas graves para la salud.
- Reglamento Sanitario Internacional revisado adoptado por la 58ª Asamblea Mundial de la Salud el 23 de mayo de 2005 y que entró en1 vigor en junio de 2007.

esa notificación como medida de prevención dirigida al control de la enfermedad transmisible y a evitar su contagio a otros. La notificación permite elaborar datos estadísticos que muestran la frecuencia en la que aparece la enfermedad transmisible, lo cual, a su vez, ayuda a los investigadores a identificar las tendencias de la enfermedad y a rastrear sus brotes, lo que ayuda a evitar o controlar brotes futuros.

En España la vigilancia de enfermedades transmisibles está regulada por el Real Decreto 2210/1995 por el que se crea la Red Nacional de Vigilancia Epidemiológica. A este reglamento se añaden la Decisión n.º 1082/2013/CE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud, y el Reglamento Sanitario Internacional. La vigilancia se sustenta en la actividad de la Red Nacional de Vigilancia Epidemiológica gestionada por el Centro Nacional de Epidemiología. La Red da respuesta a las necesidades de información de las autoridades de salud y de todos aquellos profesionales que, desde distintos ámbitos y responsabilidades, necesitan conocer la presentación, patrones de riesgo y distribución de las enfermedades transmisibles en la población al objeto de orientar las medidas de prevención y control de las enfermedades transmisibles en la población. La responsabilidad de las medidas recae en el nivel autonómico y la mayor parte de las mismas se llevan a cabo en el nivel local, que es el más cercano a donde se produce el caso o brote, pero en algunas ocasiones se precisa la intervención o coordinación de las autoridades autonómicas, nacionales o internacionales. En el pleno del Consejo Interterritorial del Sistema Nacional de Salud de 23 de julio de 2013, se aprobó el acuerdo de los nuevos protocolos de las enfermedades de declaración obligatoria de la Red Nacional de Vigilancia Epidemiológica.

En el año 2009, para la vigilancia epidemiológica se implantó en Andalucía un sistema de importación automática mediante aplicación informática de casos con sospecha de enfermedad de declaración obligatoria desde la historia clínica digital a la RedAlerta. Un estudio publicado en el Revista Española de Salud Pública en 2015[126] concluye que, si bien no sustituye la declaración manual y requiere de un proceso de verificación, el sistema de incorporación automática es útil e incrementa la exhaustividad del sistema de vigilancia epidemiológica.

Padecer una enfermedad infecciosa es motivo de estigma y de discriminación. Sobra decir que la infección por VIH es una enfermedad muy estigmatizante[127] y, por ello, con unos índices de discriminación muy elevados[128]. De ahí que las personas que la padecen

[126] ONIEVA-GARCÍA, M. Á., LÓPEZ-HERNÁNDEZ, B., MOLINA-RUEDA, M. J., CABRERA-CASTRO, N. y MOCHÓN-OCHOA, M, "Aportación de la historia clínica digital a la vigilancia de enfermedades de declaración obligatoria" en Revista Española de Salud Pública, vol. 89, núm. 5, 2015, pp. 515-522.

[127] Véase al respecto BARRANCO AVILÉS, M. C., "La incidencia de la condición de no padecer enfermedad infecto-contagiosa en los derechos de las personas con VIH", en *Revista Multidisciplinar de SIDA*, vol. 1, núm. 1, 2013, pp. 14-21.

[128] Hasta el punto de que el 5 de abril de 2017, el Congreso de los Diputados aprobó por unanimidad la toma en consideración de una proposición no de ley del Parlamento de Navarra de modificar la Ley General para la Defensa de los Consumidores y Usuarios introduciendo una disposición adicional

tienen un nivel de exigencia particularmente elevado respecto de la confidencialidad de todo lo relativo a su enfermedad. La normativa reguladora de los registros autonómicos y nacional de VIH/SIDA exigen que las notificaciones sean nominales. Esta exigencia es muy cuestionada desde las asociaciones de pacientes y piden que los registros sean anónimos. Empero, una eficaz tutela de la salud pública exige en ocasiones conocer la identidad de la persona que padece la enfermedad. La Orden de 18 de diciembre de 2000, que instituye el Sistema de Información sobre Nuevas Infecciones por VIH, así lo exige y dicha exigencia fue validada por la sentencia del Tribunal Supremo de 9 de julio de 2007. Diversas instituciones (ONUSIDA, Consejo de Europa, etc.) consideran prioritario preservar la intimidad del paciente y optan por el anonimato como regla general, de manera que solo se comuniquen o se conozcan los datos identificativos cuando sea estrictamente necesario para evitar la propagación del virus y salvaguardar la salud pública. Una respuesta equilibrada a este dilema puede consistir en que las notificaciones sean nominales, pero exigiendo de los responsables de los registros que procedan a la disociación de los datos mediante un código que permita identificar a la persona con VIH, esto es, la seudonimización, y que solo se pueda acceder a los datos identificativos por profesionales autorizados cuando sea imprescindible para evitar contagios a terceras personas.

ROMEO CASABONA y CASTELLANO ARROYO[129] entiende que la declaración no es propiamente una revelación de datos sino un "secreto compartido", ya que solo se comparten dichos datos con otros profesionales que quedan igualmente obligados al deber de secreto y a actuar en beneficio del paciente y de la colectividad.

2.3. Vigilancia en salud pública.

Propuesta de regulación:

1. Las personas públicas o privadas cederán a las autoridades sanitarias, cuando así se les requiera, los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública.

2. El acceso a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública, previa motivación por parte de la Administración que solicitase el acceso a los datos, habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona en ejercicio de sus competencias en salud pública sujeta, asimismo, a una obligación equivalente de secreto.

Comentario exegético.

---

estableciendo que "serán nulas y se considerarán no vinculantes aquellas cláusulas, condiciones o pactos que excluyan a una de las partes por tener VHI/SIDA".

[129] ROMEO CASABONA, C. y CASTELLANO ARROYO, M.ª, "La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica", en *Derecho y Salud,* núm. 1, 1993, p. 8.

Establece el artículo 12 de la LGSP que la vigilancia en salud pública es el conjunto de actividades destinadas a recoger, analizar, interpretar y difundir información relacionada con el estado de la salud de la población y los factores que la condicionan, con el objeto de fundamentar las actuaciones de salud pública, tomando en cuenta factores tales como los condicionantes sociales y las desigualdades que incidan en la salud con mediciones en el nivel individual y en el poblacional; los riesgos ambientales y sus efectos en la salud, incluida la presencia de los agentes contaminantes en el medio ambiente y en las personas, así como el impacto potencial en la salud de la exposición a emisiones electromagnéticas; la seguridad alimentaria, incluyendo los riesgos alimentarios; los riesgos relacionados con el trabajo y sus efectos en la salud; las enfermedades no transmisibles; las enfermedades transmisibles, incluyendo las zoonosis y las enfermedades emergentes; los problemas de salud relacionados con el tránsito internacional de viajeros y bienes; las lesiones y la violencia.

Comprobamos, pues, que la vigilancia en salud pública trasciende ampliamente la clásica función de vigilancia de las enfermedades transmisibles y se extiende a los condicionantes de los problemas de salud. Por tanto, aquí están muy implicadas, además de las actuaciones de salud pública, la medicina preventiva y la epidemiología. El citado artículo 12 también dispone que la vigilancia en salud pública requiere contar con unos sistemas de alerta precoz y respuesta rápida para la detección y evaluación de incidentes, riesgos, síndromes, enfermedades y otras situaciones que pueden suponer una amenaza para la salud de la población, y que las comunidades autónomas y las entidades locales asegurarán en el ámbito de sus competencias que los respectivos sistemas de vigilancia en salud pública cumplen en todo momento con las previsiones de la ley, debiendo proporcionar la información que establezca la normativa nacional e internacional, con la periodicidad y desagregación que en cada caso se determine.

Al objeto de procurar el cumplimiento de estas actividades y lograr los objetivos deseados, el artículo 40 de la LGSP conforma el Sistema de Información en Salud Pública integrado por los sistemas de información en materia de salud pública o cuya información sea relevante en la toma de decisiones en esta materia, que se creen por las distintas Administraciones sanitarias, y el artículo 41 establece que las autoridades sanitarias, con el fin de asegurar la mejor tutela de la salud de la población, podrán requerir a los servicios y profesionales sanitarios informes, protocolos u otros documentos con fines de información sanitaria, y que las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales relacionados con la salud y para su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población. Y el referido artículo también dispone que los centros y servicios sanitarios públicos y privados y los profesionales sanitarios deben ceder a la autoridad sanitaria o a los órganos competentes de las Administraciones sanitarias, los datos identificativos de los pacientes que resulten imprescindibles para la toma de decisiones cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población y así se les requiera motivadamente por razones epidemiológicas o de salud pública.

La expresión "personas públicas y privadas" contenida en el artículo 41 de la LGSP se refiere a entes u órganos (centros y servicios sanitarios públicos y privados) con independencia de que tengan o no personalidad jurídica propia, ya que aquí se trata fundamentalmente de ceder datos de los ficheros o archivos de historias clínicas electrónicas existentes en los centros sanitarios. La obligación, en nombre y representación del centro o servicio, recaería en el director o jefe correspondiente.

Tanto el artículo 9.2 i) del RGPD como el artículo 43 de la LGSP obligan a las personas que tengan acceso y traten los datos de los sistemas de información instituidos a mantener el secreto profesional. Como en el caso de la declaración de enfermedades transmisibles, estamos aquí ante un secreto compartido que se genera entre profesionales sanitarios y en el ámbito de la actividad pública sanitaria con fines de vigilancia en salud pública. ROMEO CASABONA y CASTELLANO ARROYO[130] también consideran que no se trata propiamente de revelar un secreto en sentido amplio, sino de transmitir una información médica a otros médicos y/o autoridades sanitarias para que se establezcan las medidas de prevención dirigidas al control de las enfermedades y a evitar su contagio a otros. Por otra parte, estos médicos y autoridades quedarán igualmente obligados en la salvaguarda y protección del secreto, por lo que nos encontramos, afirman, con el "secreto compartido", y no con un secreto divulgado.

2.4. Comunicación de datos de salud entre Administraciones sanitarias para el ejercicio de competencias iguales o sobre materias iguales y para fines de investigación científica.

Propuesta de regulación:

1. En la comunicación de datos entre distintas Administraciones públicas o entre diferentes entes de la misma Administración, se podrán ceder los datos identificativos de las personas sin el consentimiento del interesado para el ejercicio de competencias iguales o sobre materias iguales, y para la realización de fines estadísticos o científicos con las reservas establecidas normativamente respecto de fines científicos.

2. El acceso a los datos comunicados habrá de realizarlo, en todo caso, un profesional sanitario sujeto al secreto profesional u otra persona sujeta, asimismo, a una obligación equivalente de secreto.

Comentario exegético.

El artículo 11.2 de la LOPD enumera una serie de supuestos en los que es legítimo comunicar datos a un tercero sin consentimiento previo del interesado. Así, en lo que aquí interesa, como destinatarios de los datos cita las comunicaciones entre Administraciones públicas para el tratamiento posterior de los datos con fines

[130] ROMEO CASABONA y CASTELLANO ARROYO "La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica." en *Derecho y Salud*, vol. 1, núm. 1, 1993, p. 8.

históricos, estadísticos o científicos[131]. A su vez, el artículo 11.5 establece que "Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley", y ya conocemos que el artículo 10 impone al responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal al deber de secreto profesional respecto de los mismos y al deber de guardarlos. Ahora bien, también dispone el apartado 6 que "Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores." Con la expresión "procedimiento de disociación" la LOPD se está refiriendo a la anonimización irreversible.

Por su parte, el artículo 23.1.a) de la LGSP, rubricado "De la colaboración entre los servicios asistenciales y los de salud pública" manda a las Administraciones sanitarias intercambiar la información necesaria para la vigilancia en salud pública y sobre la situación de salud y sus condicionantes sociales y el artículo 41.2, rubricado "Organización de los sistemas de información" establece que las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población.

En este contexto, interesa citar también el artículo 21 de la LOPD que permite, sin el consentimiento del afectado, la cesión de datos (entre ellos historiales médicos) cuando las Administraciones cedente y cesionaria ejerzan sus competencias sobre las mismas materias. Al referirse el citado artículo 21 a la comunicación de datos entre Administraciones públicas alude a aquella comunicación que se da entre diferentes Administraciones públicas, lo que incluye entidades con personalidad jurídica propias vinculadas a una misma Administración (por ejemplo, entre un organismo autónomo y la Consejería de Salud[132] o entre diferentes Administraciones y Entes públicos[133]). La

[131] En materia de investigación en salud, destaca el Programa público de analítica de datos para la investigación y la innovación en salud **(PADRIS)** de Cataluña, que tiene la misión de poner a disposición de la comunidad científica los datos sanitarios relacionados para impulsar la investigación, la innovación y la evaluación en salud mediante el acceso a la reutilización y cruce de los datos sanitarios generados por el sistema sanitario integral de utilización pública de Cataluña (SISCAT). Según indica la reseña de este programa, los datos anonimizados y desidentificados serán accesibles al personal investigador de los centros de investigación acreditados por la institución Centres de Recerca de Catalunya (CERCA), los agentes del SISCAT y los centros de investigación universitarios públicos, así como la misma Administración sanitaria (por ejemplo, grupos de investigación de los planes directores del Departamento de Salud).

[132] LARIOS RISCO, D., "Historia clínica-Protección de datos-Secreto profesional", en *Guía Práctica de Derechos de los Pacientes y de los Profesionales Sanitarios,* Thomson-Reuters-ARANZADI, 2016, p. 200, pone el siguiente ejemplo: una consejería de salud requiere a una serie de hospitales para que le remitan un listado de pacientes de entre 30 y 50 años que incluya el nombre, domicilio y teléfono, para poner en marcha un programa de detección precoz del cáncer de mama.

[133] Los Colegios Oficiales de Farmacéuticos encauzan la obligación de las oficinas de farmacia de colaborar con el Servicio de Salud al que corresponda el abono del correspondiente gasto farmacéutico, mediante la ordenación de toda la información referente al mencionado gasto para su remisión al servicio de salud autonómico. Las actuaciones que el Concierto exige de los Colegios Profesionales en relación al

redacción del artículo 21 responde al principio de finalidad, según el cual los datos se recaban para una finalidad determinada, explícita y legítima. En esta misma línea finalista, el artículo 4.2 LOPD establece que "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No considera incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos."

No cabe duda, pues, que la recogida de datos de salud con fines asistenciales y su posterior uso con fines de investigación sanitaria son ejercicio de competencias en la misma materia. Entre los fines científicos se han de entender comprendidos estudios epidemiológicos o de protección de la salud pública en los que criterios científicos o técnicos exijan trabajar con datos identificativos de las personas. Igualmente, estudios de salud pública de indudable valor social de índole observacional, con riesgo mínimo, en donde la obtención del consentimiento informado sea impracticable o extremadamente costosa.

La capacidad de las Administraciones públicas sanitarias de comunicarse datos de salud sin consentimiento de los interesados, se cierra en el artículo 43 de la LGSP con estas dos determinaciones: 1ª En todos los niveles del sistema de información en salud pública se adoptarán las medidas necesarias para garantizar la seguridad de los datos; 2ª Los trabajadores de centros y servicios públicos y quienes por razón de su actividad tengan acceso a los datos del sistema de información están obligados a mantener secreto. Nos movemos, pues, en el terreno del secreto compartido.

Las cesiones o comunicaciones de datos entre Administraciones públicas habilitadas por los citados artículos de la LOPD y la LGSP, sin consentimiento del afectado, tienen encaje en las excepciones previstas en el artículo 9.2.h) e i) del RGPD (gestión de los sistemas y servicios de asistencia sanitaria y social e interés público en el ámbito de la salud pública).

2.5. Farmacovigilancia: comunicaciones a registros nominales de efectos adversos de medicamentos.

Propuesta de regulación:

1. En la comunicación de datos a los registros nominales de vacunación se incluirán los datos de identificación personal de los vacunados.

2. En la comunicación de efectos adversos al Sistema de Farmacovigilancia se identificará a la persona que los ha sufrido y el centro sanitario donde se han producido.

---

tratamiento automatizado de los datos personales contenidos en las recetas, es un supuesto típico de cesión de datos entre Administraciones públicas (Informe de la AEPD 126/03).

No será aplicable el derecho de acceso establecido en el artículo 15 del Reglamento (UE) 2016/679, de 27 de abril de 2016, por parte de la persona vacunada o de sus representantes legales a los datos personales que conciernen al vacunado existentes en los registros de efectos adversos.

3. Los profesionales sanitarios encargados del estudio, tratamiento y análisis de los datos obrantes en los registros nominales del Sistema de Farmacovigilancia, quedan sujetos al deber de secreto profesional.

Comentario exegético:

El art. 53.2 del Texto Refundido de la LGURM encomienda a los médicos, farmacéuticos, dentistas, enfermeros y demás profesionales sanitarios:

> el deber de comunicar con celeridad a los órganos competentes en materia de farmacovigilancia de cada comunidad autónoma las sospechas de reacciones adversas de las que tengan conocimiento y que pudieran haber sido causadas por medicamentos.

Igualmente, en el caso de los ensayos clínicos es obligatoria la comunicación conforme disponen los artículos 49 y 50 del Real Decreto 1090/2015, de 4 de diciembre, de ensayos clínicos con medicamentos.

En lo que hace a las vacunas no está regulado un sistema propio específico que recoja y analice los efectos adversos asociados a estos medicamentos[134]. En algunas comunidades autónomas se han creado los Registros Nominales de Vacunación[135], pero en su diseño y funciones no se ha contemplado la recogida y análisis de los efectos adversos de este tipo de medicamentos, aunque se recomienda que incorporen un sistema de información para dar soporte a la notificación y posterior investigación de las reacciones y eventos adversos asociados a las vacunas.

Disponemos de un sistema de farmacovigilancia para facilitar la recogida de información sobre los efectos adversos que pueden ocasionar los medicamentos denominado Sistema Español de Farmacovigilancia de medicamentos de uso Humano (SEFV-H). Tiene como objetivo principal reunir los casos de sospecha de reacciones adversas a medicamentos que identifican los profesionales sanitarios o los

[134] Las reacciones adversas que pueden aparecer tras la vacunación se clasifican, según la Organización Mundial de la Salud, en función de su causa, en: reacciones inducidas por la vacunación; reacciones por defectos en la calidad de la vacuna; reacciones debidas a errores de programa (durante el almacenamiento, la manipulación o la administración); reacciones debidas a ansiedad por el acto de la vacunación; reacciones coincidentes con la vacunación; y reacciones idiosincrásicas o de causa desconocida. Recientemente, el Tribunal de Justicia de la Unión Europea en respuesta a una consulta del Tribunal de Apelación de París admite que en el caso de un paciente francés puede demostrarse la relación de causalidad entre la esclerosis múltiple que sufre y la vacuna de la hepatitis B que recibió meses antes, sin que medie prueba científica.

[135] La Ponencia de Programas y Registro de Vacunaciones del Consejo Interterritorial del Sistema Nacional de Salud ha adoptado decisiones tendentes a implantar estos registros en todas las comunidades autónomas.

ciudadanos[136]. En cada comunidad autónoma existe un centro de farmacovigilancia, encargado de evaluar y registrar en una base de datos común, denominada FEDRA, los efectos adversos que se sospecha que pueden ser debidos al medicamento. La Agencia Española de Medicamentos y Productos Sanitarios actúa de coordinador del SEFV-H a través de la División de Farmacoepidemiología y Farmacovigilancia. El núcleo fundamental de trabajo del SEFV es la notificación de sospechas de reacciones adversas a través del Programa de notificación espontánea. Estas notificaciones adversas son enviadas por los profesionales sanitarios a través de unos formularios estandarizados de recogida de datos y son evaluadas, codificadas y registradas en FEDRA. La información contenida en FEDRA es evaluada periódicamente por los técnicos del SEFV-H con el fin de identificar de forma precoz posibles problemas de seguridad derivados del uso de los medicamentos (generación de señales de alerta). Dichas señales son discutidas en el Comité Técnico y trasladadas al Comité de Seguridad de Medicamentos de Uso Humano (CSMH) cuando se considere oportuno, atendiendo al procedimiento establecido en el reglamento interno del CSMH.

En algunos países, como en Estados Unidos, existe un sistema nacional específico y propio para la notificación de efectos adversos de vacunas.

La Disposición adicional primera del Real Decreto 577/2013, de 26 de julio, por el que se regula la farmacovigilancia de medicamentos de uso humano establece:

> *Protección de datos.* La regulación contenida en este Real Decreto se debe entender sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, de forma que en el tratamiento informático de los datos derivados del desarrollo de las actividades de farmacovigilancia así como su proceso electrónico, deberá quedar garantizada, conforme previene la normativa específica de aplicación, la confidencialidad, la intimidad personal y familiar de los ciudadanos y la protección de sus datos de carácter personal.

2.6. El deber de secreto compartido en el ámbito asistencial.

Propuesta de regulación:

1. Toda persona que por estar implicada directamente en la atención sanitaria del paciente junto al médico responsable o indirectamente por razón de la correcta gestión del centro sanitario (otros médicos especialistas del equipo, farmacéuticos, enfermeras, matronas, auxiliares de clínica, trabajadores sociales, administrativos, técnicos informáticos, inspectores, gestores, evaluadores y otros), acceda y conozca datos de salud de los pacientes, queda sujeta al deber de secreto.

[136] Véanse SARRATO MARTÍNEZ, L., "El control de la Administración Sanitaria sobre el medicamento puesto en circulación: aspectos problemáticos de su régimen jurídico" en *Revista Derecho y Salud,* vol. 25, núm. 1, 2015, pp. 9-60 y "Sistema de Farmacovigilancia de Vacunas" en *Atención Primaria,* vol. 43, núm. 8, 2011, pp. 447-453.

2. El acceso quedara estrictamente limitado a los datos que necesite conocer para el ejercicio de sus funciones, quedando prohibido un uso distinto al que le corresponde por sus funciones.

3. El médico de familia y el médico de medicina laboral podrán comunicarse mutuamente los datos de salud de los trabajadores que asisten al objeto de lograr un mejor conocimiento de la clínica del paciente y de la capacidad o incapacidad para desempeñar determinados puestos de trabajo.

Comentario exegético:

Siguiendo a DE LORENZO[137] es de señalar que en sus orígenes y hasta mediados del siglo XX, la práctica clínica tenía un carácter estrictamente bilateral, en el que sólo se relacionaban médico y paciente, sin que terceros "extraños" tuviesen cabida en esta relación. Pero a partir de la segunda mitad del siglo XX, en razón de su especialización, la medicina ha evolucionado hacia la práctica en equipo, hasta el punto de que actualmente el paciente es atendido por un conjunto de profesionales sanitarios, por auténticos equipos multidisciplinares en los que trabajan conjuntamente diferentes especialistas junto a personal técnico o de enfermería. Y, además, los avances tecnológicos y las labores de gestión y administración de los centros sanitarios han obligado a que otros profesionales no sanitarios accedan a la documentación clínica para el desarrollo de tareas administrativas, o para el mantenimiento de bases de datos en las que se alberga información de carácter médico, o para la evaluación de la calidad de la actividad asistencial del centro.

Dos principios enmarcan el acceso a la historia clínica: el de vinculación asistencial, que legitima el acceso a los profesionales sanitarios y al personal con funciones de inspección, evaluación, acreditación y planificación, administrativas y de gestión, y el de proporcionalidad, que limita el acceso a la finalidad para la que se recaban los datos y el uso o utilización que de ellos se puede hacer[138].

Nuestro legislador no ha desconocido esta realidad y la contempla en el artículo 16 de la LBAP posibilitando el acceso a los datos de las historias clínicas a los profesionales sanitarios del centro que intervienen en la asistencia del paciente, al personal administrativo y de gestión de los centros, pero exclusivamente respecto de los datos relacionados con el ejercicio de sus propias funciones, y al personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, en cumplimiento de sus respectivas funciones. Termina el artículo

[137] DE LORENZO, *El secreto médico derivado,* en Redacción Médica de 11 de febrero de 2013, disponible en: https://www.redaccionmedica.com/opinion/el-secreto-mdico-derivado-4970

[138] Véase MILLÁN CALENTI, R. A., "Historia clínica electrónica: accesos compatibles" en PALOMAR OLMEDA, A. y CANTERO MARTÍNEZ, J. (dirección) *Tratado de Derecho Sanitario*, Tomo I, Thomson Reuters ARANZADI, 2013, p.791.

sujetando a todas estas personas al deber de secreto[139]. Implícitamente instituye el deber de secreto compartido. Cuestión distinta es el acceso indebido por terceros a historias clínicas, donde no se genera un problema de violación del secreto profesional sino un problema seguridad en el fichero de historias clínicas.

En el mes de julio de 2017, la Comisión Central de Deontología aprobó una Declaración sobre el secreto médico, en la que se destaca la necesaria relación comunicativa entre el médico del trabajo y el de familia. FERNÁNDEZ CHAVERO afirma al respecto[140] que "urge una normativa que facilite el diálogo entre el médico de familia y del trabajo para dar un salto de calidad en la asistencia y verosimilitud de los datos de salud", y pone el siguiente ejemplo: "un conductor de autobús escolar es atendido por su médico de primaria y le comenta que es adicto al alcohol y drogas. El facultativo lo anota en su historia clínica. Posteriormente, en el reconocimiento médico de su empresa en el cuestionario, que se le hace de buena fe, es preguntado acerca de si toma alcohol o drogas. Contesta que no. El médico de empresa emite un informe donde avala la aptitud del trabajador para conducir autobuses. En este caso es obvio que se ha ocultado información que puede repercutir en la protección de terceros". Por el contrario, "si existiera un diálogo entre ambos médicos, guardando la cadena de confidencialidad, se ganaría en transparencia, fluidez en la asistencia, rapidez en el manejo de las bajas labores y el absentismo y evaluación global de una mejor clínica del paciente". De ahí el apartado 3 de la propuesta de regulación.

Por otra parte, en lo referente a la prescripción y dispensación de medicamentos, la receta médica y las órdenes de dispensación hospitalarias son documentos normalizados que suponen un medio fundamental para la transmisión de información entre los profesionales sanitarios, además de su papel como soporte para la gestión y facturación de la prestación farmacéutica que reciben los usuarios del Sistema Nacional de Salud.[141]

2.7. Registros de instrucciones previas.

Propuesta de regulación:

Las personas que en ejercicio de sus funciones accedan a los registros de instrucciones previas o voluntades anticipadas están obligadas a guardar secreto acerca de los datos que conozcan como consecuencia de dicho acceso.

Comentario exegético:

[139] Sobre accesos a la historia clínica, MARTÍ MONTESINOS, C. y PIDEVALL BORRELL, I., "Acceso a la historia clínica, …" en el libro colectivo *Autonomía del paciente, información e historia clínica (estudios sobre la Ley 41/2002, de 14 de noviembre)*, Thomson-Civitas, 2004, pp. 101-135; MILLÁN CALENTI, R., "Historia clínica electrónica: accesos compatibles", en el libro colectivo PALOMAR OLMEDA y CANTERO MARTÍNEZ (dirección) *Tratado de Derecho Sanitario,* Tomo I, Thomson-Reuters-ARANZADI, 2013, pp. 779-803.

[140] FERNÁNDEZ CHAVERO M., médico del Trabajo y vocal de la Comisión Central de Deontología de la Organización Médica Colegial en declaraciones a Diario Médico de 17 de julio de 2017.

[141] Véase GIL MEMBRADO, C., "La E-Receta: confidencialidad y proyecto de regulación" en *Derecho y Salud,* vol. 21, núm. 1, 2011, pp. 31-60.

El artículo 11 de la LBAP regula las instrucciones previas, también denominadas "voluntades anticipadas" en alguna legislación autonómica, como el documento dirigido al médico responsable en el cual una persona mayor de edad, o un menor al que se le reconoce capacidad conforme a la norma autonómica correspondiente, deja constancia de los deseos previamente expresados sobre las actuaciones médicas para cuando se encuentre en una situación en que las circunstancias que concurran no le permitan expresar personalmente su voluntad, por medio del consentimiento informado, y que deben ser tenidos en cuenta por el médico responsable o por el equipo médico que le asista en tal situación. En este documento pueden incorporarse manifestaciones para que, en el supuesto de situaciones críticas, vitales e irreversibles respecto a la vida, se evite el sufrimiento con medidas paliativas aunque se acorte el proceso vital, no se prolongue la vida artificialmente por medio de tecnologías y tratamientos desproporcionados o extraordinarios, ni se atrase abusiva e irracionalmente el proceso de la muerte. Se trata de un documento que contiene datos personales y manifestaciones relativas a la salud y asistencia sanitaria que se desea.

Existen registros de instrucciones previas en todas las comunidades autonómicas y un Registro Nacional en el Ministerio de Sanidad, Servicios Sociales e Igualdad, en los que se inscriben los documentos, su modificación, sustitución y revocación, independientemente del procedimiento de formalización empleado, con objeto de garantizar su conocimiento por los facultativos de los centros asistenciales, tanto públicos como privados.

Conforme a la normativa reguladora de los registros autonómicos tienen acceso a los registros los profesionales sanitarios que han de prestar asistencia sanitaria al otorgante del documento, que son sus principales destinatarios, el representante legal, la persona designada por el otorgante del documento para que le represente y las personas responsables del registro. El artículo 4.1 del Real Decreto 124/2007, de 2 de febrero, por el que se regula el Registro Nacional de instrucciones previas, establece que se encuentran legitimados para acceder a los asientos del Registro Nacional:

> a) Las personas otorgantes de las instrucciones previas inscritas en él.
> b) Los representantes legales de las personas otorgantes o los que a tal efecto hubieran sido designados de manera fehaciente por estas.
> c) Los responsables acreditados de los registros autonómicos.
> d) Las personas designadas por la autoridad sanitaria de la comunidad autónoma correspondiente o por el Ministerio de Sanidad y Consumo.

Como no puede ser de otra forma, el apartado 5 del citado artículo 4 establece:

> 5. Las personas que, en razón de su cargo u oficio, accedan a cualquiera de los datos del Registro nacional de instrucciones previas están sujetas al deber de guardar secreto.

Así pues, todas las personas que accedan a los datos de estos documentos a través del Registro Nacional o de los registros autonómicos deben estar legalmente obligadas a guardar secreto respecto de dichos datos. Nos situamos, por tanto, en el terreno del

secreto compartido, si bien no necesariamente la persona que acceda ha de ser un profesional sanitario.

3. Excepciones al deber de secreto: secreto divulgado.

3.1. Introito.

Se acomete seguidamente el estudio de los supuestos legalmente establecidos en los que se excepciona el deber de secreto, pero en los que la comunicación de los datos se produce entre médicos o profesionales sanitarios y terceras personas totalmente ajenas al sector sanitario: personas físicas particulares, jueces, fiscales, funcionarios judiciales que intervinieron en la tramitación de un asunto, letrados que participaron en el proceso en defensa y representación de los litigantes, defensores del pueblo, empresarios, etc. En estos casos no media una actividad sanitaria pública, sino el motivo de la comunicación de los datos es resolver un conflicto judicial, tratar de evitar un riesgo grave e inminente que amenaza a una o varias personas físicas, resolver reclamaciones extrajudiciales, etc., ámbitos estos respecto de los que difícilmente es predicable la institución del deber de secreto compartido ya que no hay el nivel de confidencia exigido normativamente para los profesionales sanitarios en el ejercicio de sus respectivas funciones en el ámbito sanitario. En estos casos, no es jurídicamente viable exigir a todas las personas que por una vía u otra pueden conocer datos personales que, a su vez, mantengan absoluta reserva de los datos que han conocido. En fin, frecuentemente personas particulares conocen datos (comunicados por un médico en aplicación de la eximente de estado de necesidad; asistencia o participación en procedimientos judiciales, particularmente en los procesos penales[142]; por comunicación de datos genéticos a un familiar biológico por razones de grave riesgo; padres o tutores a los que se le comunican datos para autorizar o no la intervención clínica a un menor maduro, la simple lectura por cualquier persona de una sentencia judicial, que son de acceso público, en las que pueden describirse datos de salud[143], etc.) y ninguna norma les obliga a mantener el secreto respecto de los datos que han conocido[144]. Estamos realmente ante el secreto divulgado.

[142] RAGUÉS I VALLÈS, R., "La trascendencia penal de la obtención y revelación de información confidencial en la denuncia de conductas ilícitas", *InDret, Revista para el Análisis del Derecho*, 3/2015, p. 19, escribe al respecto "por más que la policía, fiscales o jueces –y también los abogados o procuradores que intervienen en un procedimiento penal– tengan deberes de reserva, la práctica demuestra con incontables ejemplos que *cuando una determinada información se aporta a un procedimiento judicial existe un riesgo claro de que ésta acabe trascendiendo en mayor o menor medida*. De hecho, aunque nadie revele ilegítimamente dicha información, la mera circunstancia de que ésta se aporte a un procedimiento en el que puedan estar comparecidas numerosas partes procesales con sus respectivos abogados y procuradores, además de los funcionarios judiciales, ya supone que un número importante de personas tendrá conocimiento de la información aportada, lo que en sí mismo ya supone un menoscabo de las legítimas expectativas de reserva que pudiera tener el afectado."

[143] Se procede a la disociación de los datos personales, pero consiste en poner solo los nombres de los litigantes, sin apellidos, y la realidad es que, combinando los nombres con los demás datos y circunstancias que se describen en la sentencia, resulta extremadamente fácil identificar a las personas involucradas en el procedimiento judicial y sus datos de salud.

[144] El artículo 10 de la LOPD rubricado "Deber de secreto" establece 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 mismo."

Conforme a nuestro ordenamiento jurídico, seguidamente se enumeran las excepciones al deber de secreto que establece la legislación de forma directa o indirecta y que, además, tienen refrendo jurisprudencial y doctrinal[145], que encajan en la noción de secreto divulgado. Las circunstancias en las que legalmente se permite o se exige revelar el secreto médico a terceros son[146]:

a) Existencia de un riesgo grave para terceros: eximente de estado de necesidad.

b) Por imperativo legal:

- Expedición de certificados de nacimiento y de fallecimiento.
- Denuncia a las autoridades de delitos públicos.
- Acceso a la historia clínica con fines judiciales.
- Deber de colaborar con la administración de justicia: obligación de los profesionales sanitarios de declarar en juicio como perito o testigo.
- Vigilancia de la salud de los trabajadores.
- Asistencia a menores de edad maduros en intervenciones clínicas graves y en abortos.

c) Por directa habilitación *ex lege*:

- Comunicación de datos genéticos u otros de carácter personal obtenidos en el curso de una investigación biomédica o de muestras biológicas al objeto de evitar un grave riesgo para familiares biológicos.

Algunos de los supuestos enumerados solo surgen como consecuencia de la actividad de asistencia sanitaria, no de la actividad de salud pública. Son, por ejemplo, la expedición de certificados de nacimiento y de fallecimiento; el acceso judicial a historias clínicas para resolver asuntos de responsabilidad médica derivada de la asistencia hospitalaria o extrahospitalaria a un paciente; el conocimiento de la existencia de un riesgo grave para terceros derivado de una relación clínica o de la realización de test genéticos o muestras biológicas; la asistencia a menores de edad maduros en intervenciones clínicas graves. Otros supuestos suceden, aunque sean infrecuentes, cuando un médico o un profesional

---

Pues bien, las personas reseñadas no intervienen en ninguna fase del tratamiento por lo que no les es exigible este deber establecido con carácter general por este artículo de la LOPD. Si revelasen a un tercero los datos que les ha comunicado verbalmente el médico difícilmente encajaría la conducta en el delito de revelación de secreto tipificado en los artículos 197 a 199 del Código Penal pues no concurrirían los requisitos necesarios establecidos en esos artículos para que se produzca el delito.

[145] Sobre la justificación ética de las excepciones establecidas legalmente, véase ALTISENT TROTA, R., voz "Confidencialidad" en ROMEO CASABONA (director) *Enciclopedia de Bioderecho y Bioética,* Comares S.L., 2011, Tomo I, pp. 427-429.

[146] Hay otros intereses públicos que no se han considerado suficientes para exonerar del deber secreto a los profesionales sanitarios. Así, por ejemplo, la STS de 6 de marzo de 1989 -RJ/1989/2177- anuló el reglamento que imponía que las facturas de los médicos indicaran la actuación clínica o quirúrgica realizada por considerar que vulneraba el derecho a la intimidad del paciente. También cabe citar el artículo 11.4 de la Ley Orgánica 3/2013, de 20 de junio, de protección de la salud del deportista y lucha contra el dopaje en la actividad deportiva, que no exonera del secreto profesional, al establecer taxativamente que los médicos solo pueden informar de los tratamientos a que estén sometidos los deportistas si estos consienten expresamente.

sanitario puede resultar implicado al realizar, no una actividad de asistencia sanitaria, sino una actividad de salud pública, medicina preventiva o salud comunitaria.

Respecto del segundo grupo de supuestos, procede hacer referencia al artículo 11 de la LCCSNS en cuanto configura la salud pública como una prestación sanitaria dirigida a preservar, proteger y promover la salud de la población a través de actuaciones que comprenden la información y la vigilancia epidemiológica, la protección y promoción de la salud, la prevención de las enfermedades, la vigilancia y control de riesgos para la salud, etc., prestaciones que han de darse con carácter de integralidad a través de las estructuras de atención primaria. Son, pues, los médicos de familia y comunitaria de atención primaria conjuntamente con los epidemiólogos quienes diseñan y ejecutan programas y actuaciones de salud pública, de salud comunitaria, de medicina preventiva, dirigidas al individuo, a la familia y a la comunidad. En la ejecución de estas actuaciones y programas normalmente no se produce una relación clínico-asistencial directa con un paciente, aunque sí requiere imbricarse con los colectivos de ciudadanos a los que se dirige el programa. Pero además de las actividades dirigidas a la comunidad también las hay dirigidas al individuo y a la familia donde sí se genera una relación más personal. La vacunación, que es una prestación individual, no es una actividad asistencial sino una acción de prevención primaria, que puede producir efectos adversos, desde leves a graves, de los que pueden resultar exigencias de indemnizaciones o responsabilidades que, en su caso, terminan dirimiéndose en sede judicial. Los programas de cribado son actividades de salud pública de carácter preventivo (prevención secundaria) orientadas a la detección precoz de la enfermedad, a su diagnóstico y tratamiento temprano, que se ofrecen activamente al conjunto de la población susceptible de padecer la enfermedad, aunque no tenga síntomas ni haya demandado ayuda médica. El cribado, como la mayoría de intervenciones, produce efectos adversos de diferente gravedad y magnitud (falsos positivos, complicaciones de las pruebas diagnósticas, sobretratamiento, etc.)[147], de donde también pueden derivarse responsabilidades. En el cribado de enfermedades genéticas se realizan pruebas genéticas de las que resulta una predisposición familiar a padecer una determinada enfermedad.

En suma, la actividad de salud pública exige dar prestaciones al individuo, a la familia y a colectivos de ciudadanos, y por causa o motivo de la realización de estas prestaciones los profesionales sanitarios pueden conocer enfermedades genéticas que impliquen un riesgo grave para otros familiares, la comisión de delitos públicos o pueden ser llamados por el juez para comparecer judicialmente como peritos o testigos. Estas excepciones al deber de secreto (secreto divulgado) deben de tener un régimen jurídico propio y diferente a las del secreto compartido pues mientras de estas puede afirmarse que siguen situándose en el marco del secreto profesional, no puede afirmarse lo mismo de aquellas.

[147] Recogido del *Documento marco de cribado poblacional* aprobado por la Comisión de Salud Pública celebrada el 15 de diciembre de 2010, Ministerio de Sanidad y Política Social, pp. 3 y 15. Disponible en: http://www.msssi.gob.es/profesionales/saludPublica/prevPromocion/documentomarcoCribado.htm

Pasamos, pues, a analizar estos supuestos.

3.2. Denuncia de delitos públicos[148].

Propuesta de regulación:

1. Los profesionales sanitarios deberán denunciar a las autoridades posibles delitos públicos que afecten a la vida, a la integridad física, a la salud y a la libertad, comprendida la libertad sexual, siempre que se aprecie una intención inequívoca de comisión y la denuncia sea el último recurso para evitar el peligro. La denuncia será obligada para la evitación de un peligro futuro con la conducta de la persona, pero no en lo que se refiere a conductas delictivas tenidas en el pasado, y se limitará a los datos estrictamente necesarios para evitar el peligro. Respecto de hechos que ya no se pueden evitar prevalecerá el deber de secreto profesional.

2. La denuncia en el caso de sospecha de violencia de género o de malos tratos en menores, ancianos y personas con discapacidad[149]*, se instrumentará por medio del parte judicial de lesiones regulado en el artículo 355 de la Ley de Enjuiciamiento Criminal*[150] *siempre que a criterio del profesional sanitario con la denuncia no se comprometa la seguridad de la víctima*[151].

3. Los profesionales sanitarios encargados del estudio, tratamiento y análisis de las notificaciones y de los datos obrantes en los registros de efectos adversos, no están obligados a denunciar los delitos públicos que puedan apreciar por el conocimiento y estudio de los efectos adversos comunicados.[152]

Comentario exegético:

---

[148] Artículo 262 de la Ley de Enjuiciamiento Criminal. Delito público es el perseguible de oficio, bastando la acusación del ministerio fiscal, con independencia de que los perjudicados quieran seguir adelante con una acusación.

[149] Anexo II, 6.6.3 y Anexo IV 2.8 del Real Decreto 1030/2006, de 15 de septiembre, por el que se establece la cartera de servicios comunes del Sistema Nacional de Salud

[150] "Si el hecho criminal que motivare la formación de una causa cualquiera consistiese en lesiones, los médicos que asistieren al herido estarán obligados a dar parte de su estado y adelantos en los períodos que se les señalen, e inmediatamente que ocurra cualquier novedad que merezca ser puesta en conocimiento del Juez instructor."

[151] En Estados Unidos, en el año 2002 tan solo existía en 7 de los 50 Estados (California, Colorado, Kentucky, Mississippi, Ohio, Rhode Island, Texas) una regulación que estableciera como requisito la realización obligatoria de un parte de lesiones por parte del facultativo, pero entre ellos no existía un criterio uniforme en la forma de llevarlo a cabo. Como explicación, sostenían que la notificación obligatoria de la violencia de género pudiera afectar a la seguridad de las mujeres maltratadas o su acceso a los recursos apropiados, así como también la posibilidad de que se afectara la relación entre el médico y la víctima. Como alternativa "más adecuada" a la notificación obligatoria, se propuso ampliar y aumentar la financiación de recursos para las mujeres maltratadas y sus hijos, incluyendo refugios y hogares seguros. Datos recogidos del estudio de GONZÁLEZ DE LA PEÑA, A. S., "El secreto del profesional sanitario: Limitaciones y Singularidades.

[152] Esta determinación obligaría a modificar el artículo 263 de la Ley de Enjuiciamiento Criminal incluyendo a los profesionales sanitarios, junto a los abogados y eclesiásticos, en la exención a la obligación de denunciar delitos públicos.

El artículo 24.2 de la Constitución establece que una ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos. Pero todavía no se ha promulgado esta ley.

Actualmente, el artículo 263 de la LECrim exime a los abogados y eclesiásticos del deber de denunciar delitos, pero no a los médicos. El deber del médico de declarar presuntos delitos de los que tuviere conocimiento en el ejercicio de su profesión supone una clara, pero discutible, limitación al deber de secreto. Aquí se contraponen dos deberes: el de confidencialidad, al que claramente obliga la legislación sanitaria y el Código Penal, y el de declarar, exigido con rotundidad por el artículo 262 de la LECrim[153]. Desde la perspectiva exclusivamente legal puede sostenerse que hay una incoherencia pues, de un lado, tanto la legislación sanitaria como el artículo 199.2 del Código Penal sujetan a los profesionales sanitarios al deber de secreto sin establecer ninguna excepción por causa del conocimiento de hechos delictivos, y, de otro lado, el artículo 262 LECrim obliga a los profesionales sanitarios a denunciar delitos, conflicto que no es fácil de resolver. Por tanto, desde esta perspectiva sería oportuno modificar los artículos 262 y 263 de la LECrim incluyendo a los médicos y resto de profesiones sanitarias, junto a los abogados y eclesiásticos, en la exención a la obligación de denunciar delitos públicos[154].

Desde una visión ética, la revelación de información confidencial no está justificada sin más por conformarse como una exigencia legal en el caso de los delitos públicos pues subyace un desgarrador conflicto entre la obligación ética de guardar secreto por fidelidad y lealtad al paciente y la obligación legal de declarar, y, en atención a las circunstancias concurrentes, hecha la ponderación necesaria, bien puede prevalecer la valoración ética sobre una imposición legal. Para el médico, la lealtad debida al paciente o al ciudadano con el que se relaciona sanitariamente condicionará siempre la decisión que tome ante su obligación legal de declarar un delito o de comparecer como testigo en un proceso penal. De ahí que resulte del todo razonable eximir al profesional sanitario de la obligación impuesta por el artículo 262 de la LECrim. Y, en efecto, la doctrina[155] ha reclamado insistentemente que también se incluya a los profesionales sanitarios que

[153] Es muy conocida la Sentencia del Tribunal Supremo 778/2013, de 22 de octubre de 2013, que analiza el supuesto de un cirujano que investigó documentación de pacientes suyos y de otros médicos al detectar un posible problema sanitario en las prótesis mamarias implantadas en la clínica y lo denunció a la fiscalía. Estima el Tribunal Supremo que en relación al art. 199 CP (secreto profesional) la conducta estaría justificada por el cumplimiento de un deber (art. 20.7 CP: cumplimiento de un deber). Afirma el TS que la conducta de poner en conocimiento de la autoridad competente lo que entiende son hechos delictivos no es revelar secretos, sino cumplir con la obligación impuesta en el art. 259 y siguientes de la Ley de Enjuiciamiento Criminal (LECrim); deber de denunciar impuesto legalmente y con especial intensidad al médico en el art. 262 de la LECrim.

[154] Ahora bien, por cuanto el secreto profesional está íntimamente vinculado con el derecho fundamental a la intimidad, probablemente se entienda que esta modificación exija ley orgánica, en cuyo caso no puede hacerse mediante ley ordinaria, salvo que se le dé rango de Ley orgánica a la concreta disposición que haga la modificación.

[155] Por toda, MORALES PRATS, F., en *Comentarios al Nuevo Código Pena*l, 2.ª edición, Aranzadi, 2001, pp. 1001 y ss.

prestan asistencia sanitaria toda vez que su relación con el paciente está presidida por los principios de intimidad, de lealtad y de confidencialidad.

Pero también ha de advertirse que en el ámbito de la salud pública y la comunitaria[156] normalmente no se da esa íntima y personalísima relación entre médico y paciente en la que este revela al médico datos atinentes a su vida privada en la confianza que guardará sigilo sobre ello. No hay aquí una relación personalísima sino una relación despersonalizada, no íntima, una relación comunal entre equipo sanitario y colectivo de ciudadanos a los que se dirige el programa de salud pública, comunitaria o familiar. La relación directa con individuos y familias no es asistencial sino de carácter educativo e informativo con el fin de educarles y generarles capacidad sanitaria. En suma, no concurren las razones éticas de lealtad y confidencialidad propias de la relación clínico-asistencial que justificarían eximirles del deber de denunciar delitos públicos, como sí concurren en el abogado y en el eclesiástico y también en el profesional sanitario que presta asistencia sanitaria a pacientes.

Aceptado que en el campo de la salud pública y la comunitaria es ético denunciar delitos públicos, procede examinar qué delitos han de denunciarse. Es opinión generalizada de la doctrina penalista[157] que las conductas delictivas tenidas en el pasado y ya no evitables no deben ser objeto de denuncia por los profesionales sanitarios, debiendo prevalecer el derecho a la intimidad y, por ende, el deber de secreto. Podría entenderse comprendida aquí la exención de denunciar delitos conocidos a través de registros de efectos adversos.

De ahí que la obligación de denuncia que proponemos solo alcanzaría a la probable comisión de hechos delictivos inminentes, pero futuros. Respecto de posibles delitos futuros, la obligación que nos ocupa estaría íntimamente conectada con la excepción de estado de necesidad justificativa de que el deber de secreto pueda ceder ante situaciones en las que hay un interés prevalente -vida, integridad física, salud- al de mantener la reserva de determinada información. Y, en nuestro criterio, puede ser más razonable y coherente decantarse por que el profesional sanitario haga un uso discrecional, potestativo, de la eximente de estado de necesidad, que obligarle por determinación legal a denunciar la inminente comisión de delitos.

No obstante, probablemente esté justificada la denuncia obligatoria, no potestativa como lo es en el caso de estado de necesidad, en los casos de violencia de género y en la de menores, ancianos e incapacitados, a fin de prevenir futuras agresiones, y cuando un infectado de VIH desea intencionadamente transmitir la infección a terceros con lo que

[156] La salud comunitaria desplaza el foco desde la enfermedad al bienestar y desde la restitución de la salud a su promoción. Véase al respecto PASARÍN, I. y DIEZ, E., "Salud comunitaria: una actuación necesaria" en *Gaceta Sanitaria,* vol. 27, núm. 6, 2013.

[157] Así, HIGUERA GUIMERÁ, J. F., "El descubrimiento y la revelación de secretos" en *Actualidad Penal,* núm. 31, 2002, pp. 767 y ss.; GOMEZ RIVERO, C., voz "Secreto médico", en ROMEO CABONA (director) *Enciclopedia de Bioderecho y Bioética,* Comares S.L., 2011, Tomo I, p. 1508; GARCÍA SANZ, J El secreto profesional en el ámbito sanitario" en *Estudios Jurídico-Penales sobre Genética y Biomedicina, Libro Homenaje al Prof. Dr. D. Ferrando Mantovan*i, Dykinson, 2005, p. 470,

mantiene relaciones sexuales. Los autores que han estudiado con detenimiento la violencia doméstica se inclinan claramente por la opción de que el profesional sanitario emita el correspondiente parte de lesiones, ya que consideran que el papel de los profesionales sanitarios en este ámbito es clave en la detección y abordaje de este tipo de violencia[158]. Participamos de este criterio pues consideramos que el bien protegido con tal acción -emitir el parte de lesiones- es muy superior al bien que representa la confidencialidad/secreto. En cualquier caso, ante este tipo de violencia, todos los ordenamientos jurídicos están reforzando los resortes jurídicos y normativos a fin de prevenirla y evitarla. Así, en nuestro país, el articulo 544ter.2 de la LEcrim, introducido en el año 2003, establece que, sin perjuicio del deber general de denuncia previsto en el artículo 262, las entidades u organismos asistenciales, públicos o privados, que tuvieran conocimiento de la presunta comisión de un delito o falta contra la vida, la integridad física o moral, libertad sexual, libertad o seguridad, de las personas mencionadas en el artículo 173.2 del Código Penal (cónyuge, pareja, familiares convivientes, personas con discapacidad, etc.) deberán ponerlo inmediatamente en conocimiento del juez de guardia o del ministerio fiscal con el fin de que se pueda incoar el procedimiento para la adopción de la orden de protección

Conforme al artículo 355 de la LECrim, el médico debe emitir un parte de lesiones siempre que asista a un sujeto que presente una lesión física o psicológica, para comunicar la situación a la autoridad judicial. Se considera que el parte de lesiones está íntimamente conectado con la protección de las víctimas de la violencia de género y de malos tratos[159] y que puede ser utilizado como medio de prueba adecuado. El Decreto 3/2011, de 11 de enero, de la Junta de Andalucía, que crea y regula el modelo de parte al Juzgado de Guardia para la comunicación de asistencia sanitaria por lesiones producidas en esa Comunidad Autónoma, define las lesiones como "todo daño o detrimento de la integridad física o mental de una persona causado por cualquier medio o procedimiento que pueda motivar una posible causa judicial, bien porque la persona lesionada lo declare o porque haya signos o síntomas claros para sospecharlo."

En todo caso, entendemos que el deber del profesional sanitario de emitir un parte de lesiones debe quedar limitado a los casos de violencia de género y en la de menores, ancianos e incapacitados. Empero, no puede obviarse que la remisión de una denuncia por violencia de género o de malos tratos sin el consentimiento de la víctima y la falta de declaración de la víctima en contra del agresor puede conducir a una resolución de sobreseimiento. Por ello, es importante conocer y escuchar a la víctima, y siempre que sea posible consensuar con ella la remisión al juzgado de la denuncia[160]. Hacerlo en

[158] Así, por ejemplo, MONTESINOS GARCÍA, A., "Los partes médicos de lesiones en los procesos por violencia de género" en *Actualidad del Derecho Sanitario*, núm. 240, 2016, p. 769.

[159] Véase en este sentido, GARCÍA CALVO, T. y OSUNA, E., "Eficacia jurídica de la actuación de los profesionales sanitarios en la protección de la víctima de violencia de género", en *Salud y Derecho*, vol. 26 extraordinario, XXV Congreso 2016, pp. 221-228.

[160] A pesar de alcanzarse un consenso con la víctima, esta cuestión sigue siendo delicada. Al respecto, MARTIN AYALA, D. y PONCE GARCÍA, R., "Obligación de denunciar versus prueba de cargo de la víctima en los delitos de violencia de género", en *Noticias Jurídicas* de 2 de junio de 2016, escriben que "no es nuestra intención evitar que se presenten denuncias o que queden impunes casos de agresión a una

contra de su voluntad plantea problemas éticos en cuanto supone un quebranto del deber de secreto. También podría comprometer la seguridad de la víctima en cuyo caso podría ser ético y legal no hacer la denuncia (de la denuncia se podría derivar un mal mayor del que se trata de evitar).

A modo de recapitulación de estos comentarios podemos sostener que nos encontramos ante una cuestión con dos caras que demandan respuestas distintas. De un lado, hay absoluto consenso doctrinal en que los profesionales sanitarios deben quedar exentos de la obligación de denunciar delitos públicos que ya se han cometido y no se pueden evitar, así como de los que puedan conocer a través de los registros de efectos adversos como garantía ineludible de la indemnidad que ha de presidir estos registros. De otro lado, también hay general consenso doctrinal en mantener la denuncia obligatoria, no potestativa, respecto de previsibles delitos futuros de violencia de género y doméstica, ya que constituye un elemento clave para una efectiva política de prevención. Habría, pues, que modificar el artículo 262 LECrim. contemplando esta realidad.

3.3. Deber de colaborar con la administración de justicia: obligación de los profesionales sanitarios de declarar en juicio como perito o testigo.

Propuesta de regulación:

1. Los profesionales sanitarios quedan obligados a declarar como peritos o testigos en los términos que establece la legislación procesal.

2. Cuando el profesional sanitario actúe como testigo y tenga el deber de guardar secreto respecto de hechos por los que se le interrogue, lo manifestará razonadamente y el juez o tribunal, considerando el fundamento de la negativa a declarar y ponderando el derecho a la intimidad del paciente frente al derecho a obtener una protección jurídica efectiva de las partes, resolverá, mediante providencia, lo que proceda en Derecho. Si el testigo quedare liberado de responder, se hará constar así en el acta[161].

3. Los profesionales sanitarios encargados del estudio, tratamiento y análisis de las notificaciones y de los datos obrantes en los registros de efectos adversos, se acomodarán al siguiente estatuto:

a) Quedan sujetos al deber de secreto profesional. Este deber cederá exclusivamente respecto de aquellos datos relevantes que tengan que ser utilizados en un proceso penal

---

mujer, pero sí llevar a una reflexión sobre este tema, ya que, suele ser bastante frecuente que una mujer, tras ser aconsejada y asesorada, presente denuncia en sede policial o en el Juzgado, "casi obligada" por distintas personas, como agentes o profesionales implicados en materia de violencia de género. Y que posteriormente, tras pasar el trance de las distintas declaraciones que tiene que hacer tanto en sede policial, como en sede judicial, se encuentre con distintos profesionales que cuestionan la veracidad de las mismas, produciéndole a la víctima una sensación de falta de credibilidad en su testimonio, teniendo que demostrar la veracidad de sus declaraciones, convirtiéndose en vulnerable desde el punto de vista del Derecho."

[161] Inspirado en el artículo 371 de la Ley de Enjuiciamiento Civil.

siempre y cuando el órgano judicial competente decida previamente que los mismos constituyen indicios de la comisión de un delito que no podrían obtenerse por ningún otro medio.

b) Cuando deban actuar como perito o testigo en un proceso judicial penal, manifestará razonadamente al juez o tribunal su deber de guardar secreto respecto de hechos por los que se le interrogue, y el órgano judicial considerando el fundamento de la negativa a declarar y ponderando el deber legal de secreto profesional frente al derecho a obtener una protección jurídica efectiva de las partes, resolverá, mediante providencia, lo que proceda en Derecho. Si el testigo quedare liberado de responder, se hará constar así en el acta.

Comentario exegético:

El artículo 9.2. f), del RGPD permite el tratamiento de datos de salud sin consentimiento del interesado cuando los tribunales actúen en el ejercicio de su función judicial. En este supuesto se ceden o comunican datos de salud a jueces y tribunales con quebranto del deber de secreto, y los órganos judiciales, a su vez, tratan esos datos. Aquí también el RGPD implícitamente exime del deber de secreto a los profesionales u órganos administrativos que ceden los datos, pero no sujeta expresamente a los órganos judiciales al deber de secreto, ello por cuanto la UE no tiene competencias en materia judicial pues corresponde a los Estados miembros con el carácter de exclusiva la competencia de ordenación de sus sistemas judiciales. Acudiendo, por tanto, a nuestro propio ordenamiento, resulta que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ), habilita a los jueces y tribunales a excepcionalmente acordar el carácter secreto de sus actuaciones (artículo 232.2) y a que sus deliberaciones sean secretas (artículo 233). También establece que el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la oficina judicial, se someterán a lo dispuesto en la LOPD y su normativa de desarrollo (artículo 236bis) y ya conocemos que el artículo 10 de la LOPD, rubricado deber de secreto, dispone 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 mismo.

Empero, no puede obviarse que en el ámbito judicial son públicas las actuaciones judiciales (artículo 120.1 de la Constitución y artículo 232 de la Ley Orgánica del Poder Judicial) y, normalmente, se practican en audiencia pública las diligencias de prueba y las vistas de los pleitos (excepcionalmente, por razones de orden público y de protección de los derechos y libertades, los jueces y tribunales, mediante resolución motivada, pueden limitar el ámbito de la publicidad y acordar el carácter secreto de todas o parte de las actuaciones), por lo que generalmente es inevitable el conocimiento de datos privados por cualquiera que hubiera asistido a las actuaciones desplegadas en

un pleito. Por tanto, puede afirmarse que en el ámbito judicial conviven el secreto compartido con el secreto divulgado.

En lo que hace a la práctica de las pruebas (pericial o testifical) el artículo 60.4 de la Ley de la Jurisdicción Contencioso-Administrativa se remite a la Ley de Enjuiciamiento Civil, y el artículo 289.1 de esta establece que "las pruebas se practicarán contradictoriamente en vista pública, o con publicidad y documentación similares si no se llevara a efecto en la sede del tribunal." El artículo 360 de la Ley de Enjuiciamiento Civil establece que la declaración de los testigos es oral prestada en un acto presidido por la oralidad. En la pericial el dictamen es por escrito, pero en los juicios abreviados[162] se desarrolla en la vista oral.

Centrándonos ya en las declaraciones de los médicos como peritos o testigos, señalar que conforme a los artículos 259 y 262 LECrim el profesional sanitario queda obligado a efectuar declaraciones cuando actúa como perito, y que el artículo 410 LECrim le impone implícitamente la obligación de declarar como testigo ya que el art. 417 de dicho texto legal no incluye al médico entre los profesionales o personas a los que exime de la obligación de testificar por razón del secreto profesional, como es el caso de los abogados y eclesiásticos. Conforme a la sentencia del TS 734/2015, de 3 de noviembre, el facultativo debe informar en el acto del juicio sobre los aspectos periciales (en el caso enjuiciado, conclusiones sobre padecimientos psíquicos), pero no se le debe preguntar si el paciente le relató algo sobre los hechos enjuiciados; ni debe contestar a cuestiones de ese tenor (los ámbitos más frecuentes son: psiquiatría, accidentes de tráfico, violencia doméstica y de género).

Algún sector doctrinal postula que se incluya a los médicos entre los profesionales eximidos de la obligación de testificar en razón de que existe una relación de confianza entre médico y paciente similar a la de abogado y cliente. Incluso se defiende una interpretación de la legalidad vigente que eximiría al profesional sanitario de la obligación de declarar en juicio[163]. Una sentencia del Tribunal Supremo de Estados

[162] Hasta 30.000 €: artículo 78 LJCA)

[163] GARCÍA SANZ, J, "El secreto profesional en el ámbito sanitario" en *Estudios Jurídico-Penales sobre Genética y Biomedicina, Libro Homenaje al Prof. Dr. D. Ferrando Mantovan*i, Dykinson, 2005, p. 473, escribe al respecto: "A la vista de la regulación actual, es discutible la obligación legal de testificar acerca de datos de la intimidad del paciente que conoce de la relación profesional con él. Al respecto, hubiera sido necesario que la reforma del CP de 1995 hubiera estado acompañada de una reforma de la LECrim en esta materia, ya que parece injustificado que, a diferencia de otros profesionales, el médico se halle obligado a efectuar cuantas declaraciones les exija la Administración de Justicia en el proceso penal. No obstante, cabría entender que la introducción del art. 199.2 CP permite una interpretación integradora del art. 417 LECrim. Para ello, cabe recurrir a la aplicación de los principios generales que informan las causas de justificación, debiendo ponderar en cada caso los bienes implicados. En este sentido, el derecho a la intimidad debe ser preferente sobre el deber de denunciar o testificar cuando se refiera a datos del pasado (por ejemplo, el paciente le confiesa que se sometió a un aborto ilegal en el pasado). En cambio, cuando se refiera al comportamiento futuro del paciente que pueden lesionar o poner en peligro bienes de otras personas (por ejemplo, le revela a su psiquiatra que en los próximos días va a matar a alguien) el médico estará obligado a revelar el secreto. En definitiva, el médico puede negarse a declarar como testigo o a actuar como perito, en el caso de que suponga la revelación de datos que haya obtenido en su relación profesional con el paciente, salvo que esté en peligro la vida o derechos fundamentales de otra persona que debieran prevalecer frente a la intimidad del paciente. No obstante, reiteramos la necesidad

Unidos de América de 13 de junio de 1996 declaró que "psiquiatras, psicólogos y psicoterapeutas están exentos de declarar sobre lo que su paciente les ha comunicado durante el tratamiento". A juicio del Tribunal "la efectividad del tratamiento depende de la atmósfera de confidencia y confianza en la que el paciente accede a hacer un descubrimiento franco y completo de los hechos, sus emociones, recuerdos y temores". El privilegio de estos profesionales se concibe como un servicio al interés público, pues garantizan un adecuado tratamiento a los individuos que sufren un trastorno emocional o mental.[164]

En el ámbito de la salud pública también se producen actos médicos individualizados. Son los casos de vacunaciones y de la realización de pruebas en cribados poblacionales (ambas son una prestación individual no asistencial sino de prevención primaria o secundaria), que pueden producir efectos adversos, desde leves a graves, de los que pueden resultar exigencias de indemnizaciones o responsabilidades que, en su caso, terminan dirimiéndose en sede judicial. Ahora bien, en la medida en que en estas prestaciones no se genera una relación médico-enfermo sino médico-persona sana, es improbable que la persona revele al médico datos de su vida privada que obliguen al secreto como ocurre en la relación clínica con un enfermo que demanda ayuda para curarse o mejorar. En el resto de actuaciones de salud pública también ocurre algo similar a lo comentado sobre la obligación de denunciar delitos públicos. Generalmente no se da la relación de confianza y lealtad entre médico y paciente justificativa de que el deber de secreto prevalezca sobre la obligación de declarar en juicio. Por ejemplo, a propuesta de los profesionales sanitarios que tienen funciones de prevención y protección de la salud de la población, las autoridades sanitarias para proteger la salud pública pueden adoptar medidas cautelares coercitivas sobre personas o cosas de las que puede derivarse una responsabilidad patrimonial de la Administración sanitaria, cuya existencia y, en su caso, la indemnización, se determinarán en el correspondiente proceso contencioso-administrativo[165]. Pues bien, en estos casos no parece existir inconveniente alguno de carácter ético para que médicos de familia y comunitaria o epidemiólogos acudan a juicio para declarar como peritos o testigos, particularmente como peritos) pues no están constreñidos por un deber de secreto basado en la lealtad y confidencialidad médico-paciente ya que no ha existido tal relación.

---

de que se desarrolle el art. 24 CE y se dote de una regulación pormenorizada y coherente del secreto profesional en el proceso penal, que tenga en cuenta las singularidades de esta profesión que supone el conocimiento de datos de la esfera más íntima del sujeto (vida sexual…), de modo que se delimite de forma clara y razonable los casos en los que el sujeto está obligado a declarar ante la Administración de Justicia hechos que ha conocido como "confidente necesario" en su relación profesional con el paciente."

[164] Recogida por ALVAREZ-CIENFUEGOS SUÁREZ, J. M.ª en su trabajo "Secreto médico y confidencialidad de los datos sanitarios": disponible en:
http://www.medynet.com/usuarios/jraguilar/secreto%20medico.htm

[165] Sobre esta temática, véase DOMÉNECH PASCUAL, G., "La responsabilidad patrimonial de la Administración derivada de la adopción de medidas cautelares" en *Revista Española de Derecho Administrativo,* núm. 125, 2005, pp. 65-99, donde expone diversos ejemplos de procedimientos de responsabilidad patrimonial seguidos por la adopción de medidas cautelares en defensa de la salud pública.

En lo que hace a los registros de efectos adversos, LIBANO BERISTÁIN[166], ha resaltado que los profesionales encargados del análisis de causa raíz llevan a cabo un estudio detallado de los hechos relacionados con el evento adverso y pueden llegar a extraer conclusiones enormemente valiosas de cara a la imputación y eventual condena de un profesional sanitario, y asimismo realizan un examen exhaustivo del comportamiento de cada uno de los sujetos intervinientes en relación con el acto sanitario analizado, pudiendo alcanzar conclusiones fidedignas respecto al ajuste a la *lex artis*. De ahí que sean profesionales especialmente capacitados para intervenir en un proceso judicial como peritos o testigos. Pues bien, en lo atinente al apartado 3.b) de la propuesta de regulación, esto es, acudir como testigo o perito a un proceso judicial, seguimos la recomendación que hace el informe "*El establecimiento de un sistema nacional de notificación y registro de incidentes y eventos adversos en el sector sanitario: aspectos legales*"[167], de tomar como referencia el artículo 371 de la Ley de Enjuiciamiento Civil ya que entiende, opinión que compartimos, que modula con más acierto la obligación de los profesionales sanitarios de declarar como perito o testigo.

3.4. Cribados: detección de enfermedades que impliquen un grave perjuicio para la salud de familiares biológicos.

Propuesta de regulación:

Ante la información obtenida de un análisis genético, de muestras biológicas u otras pruebas realizadas en el curso de un cribado poblacional, a pesar de la oposición del sujeto se podrá informar a un familiar próximo o a un representante cuando, según criterio del médico responsable, sea necesario para evitar un grave perjuicio para la salud de familiares biológicos, previa consulta, en su caso, del correspondiente comité de ética asistencial. En todo caso, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades.

Comentario exegético:

El artículo 20.1 de la LGSP define el cribado como aquella actividad orientada a la detección precoz de la enfermedad, su diagnóstico y tratamiento temprano, que se ofrece activamente al conjunto de la población susceptible de padecer la enfermedad, aunque no tenga síntomas ni haya demandado ayuda médica. El cribado implica practicar pruebas diagnósticas, lo que cobra especial relevancia en el campo de las

[166] LIBANO BERISTÁIN, A "Gestión de riesgos y sistemas de notificación de eventos adversos. Análisis técnico-jurídico del modelo español", en PALOMAR OLMEDA, A. y CANTERO MARTÍNEZ, J. (dirección) *Tratado de Derecho Sanitario,* vol. II, Thomson Reuters Aranzadi, 2013, pp. 349-374.

[167] El establecimiento de un sistema nacional de notificación y registro de incidentes y eventos adversos en el sector sanitario: aspectos legales. Informe. Madrid: Ministerio de Sanidad y Política Social; 2009, pp. 94-95. Se razona en el informe que "El interés de dicha disposición radica en que constituye un antecedente merecedor de ser tenido en cuenta en el conjunto de propuestas de *lege ferenda* que podrían diseñarse, de forma alternativa o complementaria, para el cambio de la normativa procesal penal, que permitiera lograr la indemnidad de datos suministrados a un eventual sistema de notificación de eventos adversos, así como la exención testifical de los miembros de comisiones técnicas encargadas de las Análisis de Causas Raíz (ACR)."

enfermedades genéticas ya que algunas son congénitas, es decir, se nace con ellas, aunque pueden tardar años en manifestarse, incluso cuando el paciente ya es adulto (por ej. algunas cardiopatías). Los cribados genéticos y registros genéticos derivados de las pruebas practicadas son apropiados para trastornos que tengan efectos potencialmente graves e impliquen un riesgo grave para familiares biológicos cuyas complicaciones puedan prevenirse.

Los cribados genéticos, conforme señala ABELLÁN[168], constituyen una herramienta para desarrollar epidemiología genética, dirigida a estudiar los factores genéticos implicados en las enfermedades complejas. El conocimiento de la distribución de los alelos de los genes (de sus formas) en distintas poblaciones contribuye a la investigación de los factores genéticos que predisponen o protegen frente a ciertas enfermedades, y puede ser útil en orden a su prevención o para desarrollar nuevos tratamientos basados en el conocimiento científico sobre esa enfermedad. La LIB define en su artículo 3.g) el cribado genético como "el programa de salud pública, dirigido a la identificación en individuos de determinantes genéticos, para los cuales una intervención médica precoz pudiera conducir a la eliminación o reducción de la mortalidad, morbilidad o discapacidades asociadas a tales determinantes."

En los cribados genéticos parece que, de entrada, debe respetarse el derecho a la confidencialidad del sujeto, pero ahí surge el dilema ético. Si el sujeto no consiente que se comunique la información obtenida a familiares, puede haber algunos que desconozcan el riesgo de ser portadores de la enfermedad, negándoles la oportunidad de conocer los medios disponibles para modificar las posibles consecuencias, y si se les comunican los datos obtenidos se viola el deber de secreto profesional.

Relata GÓMEZ RIVERO[169] que la doctrina norteamericana y australiana, partiendo del hecho de que el dato genético es común a otros familiares, defiende que ese dato pierda como referente de su titularidad a la persona individual sobre la que se ha practicado el análisis para obtener el dato genético, para pasar a adquirir una titularidad familiar, lo que, sin más, posibilitaría la comunicación de los datos a la familia biológica. A pesar de la razonabilidad de esta posición doctrinal, no es así como se ha tratado el tema en nuestro ordenamiento jurídico. De entrada, revelar el dato genético a un familiar sin el consentimiento del afectado, entraría en la lógica de la eximente de estado de necesidad[170], pero, como apunta esta autora, le faltarían dos requisitos imprescindibles para instrumentarlo por este cauce: no hay un riesgo inminente y tampoco un riesgo

[168] ABELLÁN, F., "Claves bioéticas y jurídicas de los análisis y cribados genéticos con fines asistenciales y de investigación, y tratamiento de datos genéticos" en el libro colectivo SÁNCHEZ-CARO J.y ABELLÁN F. (coord.) *Investigación biomédica en España: aspectos bioéticos, jurídicos y científicos*, Editorial Comares, 2007, p. 229.

[169] Voz "Secreto profesional" en ROMEO CASABONA (director) *Enciclopedia de Bioderecho y Bioética,* Tomo II, Editorial Comares S. L., 2011, pp. 1510-1511.

[170] El art. 20.5 del Código Penal establece que no incurrirá en responsabilidad penal: "El que, en estado de necesidad, para evitar un mal propio o ajeno lesione un bien jurídico de otra persona o infrinja un deber siempre que concurran los siguientes requisitos: 1. Que el mal causado no sea mayor que el que se trate de evitar".

futuro cierto. De ahí que nuestro legislador haya optado por habilitar *ex lege* al profesional sanitario a revelar el secreto. En efecto, la LIB (artículos 4.5 y 49.2[171]), sancionan el derecho a no saber y, en consecuencia, la imposibilidad de que el paciente, al no conocerla, transmita a terceros información que pueda resultar de interés para ellos, pero como contrapartida a este derecho a no saber prevé expresamente la posibilidad de que el profesional sanitario comunique los datos genéticos a familiares cuando el paciente tuviera una condición transmisible (por ejemplo, a la descendencia) que suponga un riesgo grave para la salud de los mismos, o exista una predisposición familiar a padecer una determinada enfermedad[172]. Por su parte, el Código de Deontología Médica autoriza a revelar el secreto "*si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo*" (artículo 30.1.c).

La LBAP no contempla expresamente este supuesto a efectos de exonerar al profesional sanitario de su deber de secreto, aunque sí contempla implícitamente esta realidad. En efecto, su artículo 9.1 establece que "La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso." Así pues, este precepto sanciona el derecho a no saber, que consiste básicamente en el reconocimiento de la voluntad de un sujeto de no ser informado sobre aspectos que afectan a su salud[173], y, en consecuencia, la imposibilidad de que el paciente, al no conocerla, transmita a terceros información que pueda resultar de interés para ellos. Cierto que este artículo no dispone expresamente nada en cuanto a la eventualidad de que, ante la renuncia a saber, sean informadas las personas vinculadas al paciente por razones familiares o de hecho, y cabría afirmar que esta posibilidad está vetada por el artículo 5.1 LBAP en cuanto solo permite comunicar a un tercero datos cuando el paciente lo autorice. Sin embargo, no procede hacer una interpretación literalista de estos artículos. Entendemos que, en cualquier caso, es

[171] Artículo 4.5: *Toda persona tiene derecho a ser informada de sus datos genéticos y otros de carácter personal que se obtengan en el curso de una investigación biomédica, según los términos en que manifestó su voluntad. El mismo derecho se reconoce a la persona que haya aportado, con la finalidad indicada, muestras biológicas, o cuando se hayan obtenido otros materiales biológicos a partir de aquéllos. Se respetará el derecho de la persona a decidir que no se le comuniquen los datos a los que se refiere el apartado anterior, incluidos los descubrimientos inesperados que se pudieran producir. No obstante, cuando esta información, según criterio del médico responsable, sea necesaria para evitar un grave perjuicio para su salud o la de sus familiares biológicos, se informará a un familiar próximo o a un representante, previa consulta del comité asistencial si lo hubiera. En todo caso, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades*.
Artículo 49.2: *Cuando el sujeto fuente haya ejercido el derecho a no ser informado de los resultados de un análisis genético sólo se suministrará la información que sea necesaria para el seguimiento del tratamiento prescrito por el médico y aceptado por el paciente. Cuando esta información sea necesaria para evitar un grave perjuicio para la salud de sus familiares biológicos, se podrá informar a los afectados o a su representante.*

[172] Véase el interesante estudio que hace SANCHEZ CARO, J. sobre la revelación de la información a los parientes consanguíneos en función de la aplicación de los principios de beneficencia, de autonomía, de justicia, y de las virtudes hipocráticas, en SÁNCHEZ-CARO J. y ABELLÁN, F. "Información genética y Derecho" en *Medicina Personalizada. Aspectos científicos, bioéticos y jurídicos,* Fundación Salud 2000, 2014, pp. 137-151.

[173] Véase ARCOS VIEIRA, M.ª L., "Consentimiento no informado: reflexiones en torno a la existencia de un "Derecho a no saber" aplicado a la información clínica.", en ARCOS VIEIRA, M.ª L. (directora) *Autonomía del paciente e intereses de terceros: límites,* Thomson-Reuters-ARANZADI, 2016, p. 62.

factible ética y jurídicamente la posibilidad de que el médico comunique los datos a un tercero sin el consentimiento del sujeto cuando concurren razones suficientes (riesgo grave), conozca o no los datos. El procedimiento a seguir sería, en primer lugar, consensuar con el sujeto el momento y forma en el que transmitirá a los familiares consanguíneos la información y, en segundo lugar, ante la negativa a hacerlo, es cuando estará legitimada una actuación de revelación del secreto. Ello por cuanto el derecho a no saber y a que no se comuniquen a un tercero datos personales no son derechos absolutos y no conlleva de ninguna manera el derecho a que los demás tampoco sepan[174].

Como ha puesto de manifiesto GÓMEZ SÁNCHEZ[175], estos límites al deber de secreto responden a la pretensión de que el reconocimiento de un derecho no lleve, de facto, a una situación de abuso o de uso antisocial del derecho. Resalta que estas medidas tienen como objetivo principal proteger el ejercicio libre de otros derechos o de valores, principios y bienes colectivos igualmente reconocidos por el ordenamiento jurídico. En suma, el derecho a no saber o a que no se conozca por otros datos personales no puede imponerse a derechos fundamentales de un tercero como la vida, la integridad física o la protección de su salud. La protección de estos bienes justifica sobradamente quebrantar el deber de secreto.

Los comités de ética asistenciales pueden y deben tener aquí bastante protagonismo como órganos consultivos al objeto de valorar que el bien a proteger con la ruptura del secreto es superior al bien de la intimidad del paciente que protege el secreto.. Su autorizada opinión es un aval para el médico y en caso de ser favorable a la ruptura del secreto refuerza y legitima la decisión de este de romper el secreto profesional.

3.5. Existencia de un riesgo grave para terceros: eximente de estado de necesidad.[176]

Propuesta de regulación:

1. Amparados en la eximente de estado de necesidad y al objeto de proteger la salud, la vida o la integridad física de las personas, en cuanto son bienes jurídicos superiores al de la intimidad, los profesionales sanitarios podrán quebrantar su deber de secreto profesional e informar a terceras personas o, en su caso, a la empresa o a las autoridades competentes, de la enfermedad, padecimiento, actitudes o intenciones de un paciente o de un trabajador particularmente en los siguientes supuestos[177]*:*

---

[174] Véase en este sentido, FEITO GRANDE, L., "Aspectos bioéticos relacionados con la medicina personalizada" en el libro colectivo SÁNCHEZ-CARO J. y ABELLÁN, F., *Medicina personalizada. Aspectos científicos, bioéticos y jurídicos,* Fundación Salud 2000, 2014, pp. 123-124.

[175] GÓMEZ SÁNCHEZ, Y., voz "Derecho a no saber" en ROMEO CASABONA, C. M.ª (director) *Enciclopedia de Bioderecho y Bioética,* Tomo I, Comares, S. L., 2011, pp. 597-599.

[176] Sobre esta institución véase CUESTA AGUADO, P., "Estado de necesidad: estructura normativa y naturaleza jurídica", en *Revista Aranzadi de Derecho y Proceso Penal,* núm. 17/2007, 1.

[177] La ruptura del deber de secreto no solo estaría legalmente amparada, sino que también será éticamente permisible. Véase al respecto las consideraciones expuestas por FERNÁNDEZ RUIZ-GÁLVEZ, E., "Intimidad y confidencialidad en la relación clínica", en *Persona y Derecho,* vol. 69/2, 2013, p. 96. El

a) cuando el trabajador pertenezca a profesiones que implican riesgos colectivos y, por causa de los reconocimientos médicos que corresponde hacer a los trabajadores, tenga razones fundadas de que pueda provocar inminentemente una catástrofe.
b) cuando como consecuencia de la relación clínica con el paciente tenga razones fundadas para temer una inminente agresión física a una o varias personas, o cometer abusos o agresiones sexuales a menores u otras personas vulnerables por razón de su edad, enfermedad, discapacidad o situación, o contagiar una enfermedad grave a otra persona.
c) Ante la renuncia del paciente a recibir información sobre su estado de salud, cuando, según criterio del médico responsable, esa información sea necesaria para evitar un grave perjuicio para la salud de terceros o de la colectividad.

2. Sólo en circunstancias extraordinarias que comporten un peligro cierto para la vida o la salud del hijo podrá revelarse la identidad de los donantes de gametos y preembriones utilizados en la reproducción humana asistida por el director o el jefe de los centros y servicios sanitarios autorizados, siempre que dicha revelación sea indispensable para evitar el peligro. Dicha revelación no implicará en ningún caso publicidad de la identidad de los donantes.[178]

3. La información se facilitará en su caso después de que el facultativo haya hecho un juicio de idoneidad-necesidad-proporcionalidad de la medida. Tendrá derecho a solicitar el asesoramiento del comité de ética asistencial correspondiente.

4. La información se dará siempre restringida a lo estrictamente necesario.

5. Como medida preventiva del conflicto ante la posible necesidad de quebrantar el deber de secreto, el profesional sanitario informará a este tipo de pacientes de cuáles son los límites del secreto médico e incorporará en el documento de consentimiento informado una explicación de dichos límites a fin de que el paciente esté informado a ser posible desde el inicio de la relación clínica o asistencial.

Comentario exegético:

El "estado de necesidad" es un principio jurídico eximente de responsabilidad por el que una persona, para proteger un bien jurídico y evitar un mal ajeno que suponga un peligro actual, inminente, grave, injusto, ilegítimo, e inevitable de otra forma legítima (en nuestro caso una lesión del derecho a la protección de la salud, a la vida, o a la integridad física de un tercero), menoscaba otro bien jurídico (lesión del derecho a la intimidad o a la protección de datos personales) generando un daño menor al que intenta evitar, siempre y cuando el mal que intenta evitar no haya sido provocado intencionadamente por el propio sujeto y este no tenga obligación de sacrificarse por

Código de Deontología Médica considera ética la revelación del secreto cuando, con su silencio, el médico diera lugar a un perjuicio para otras personas.

[178] Adaptado del artículo 5.5 de la Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida.

razón de su oficio o cargo. El artículo 20.5º del Código Penal normativiza este principio con las notas señaladas, si bien es un principio aplicable en todos los ordenamientos jurídicos.

La LBAP y el RGPD no contemplan expresamente este supuesto a efectos de exonerar al profesional sanitario de su deber de secreto cuando tratan las excepciones al requisito de previo consentimiento del interesado. Por el contrario, el Código de Deontología Médica sí autoriza a revelar el secreto "*si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo*" (artículo 30.1.c). Lo que sí hace la LBAP es contemplar implícitamente esta realidad. En efecto, su artículo 9.1 establece que "La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso." Así pues, este precepto sanciona el derecho a no saber, que consiste básicamente en el reconocimiento de la voluntad de un sujeto de no ser informado sobre aspectos que afectan a su salud[179], y, en consecuencia, la imposibilidad de que el paciente, al no conocerla, transmita a terceros información que pueda resultar de interés para ellos. Cierto que este artículo no dispone expresamente nada en cuanto a la eventualidad de que, ante la renuncia a saber, sean informadas las personas vinculadas al paciente por razones familiares o de hecho, y cabría afirmar que esta posibilidad está vetada por el artículo 5.1 LBAP en cuanto sólo permite comunicar a un tercero datos cuando el paciente lo autorice. Sin embargo, no parece que proceda hacer una interpretación literalista de estos artículos. Entendemos que la expresión *limitada* del primer inciso del artículo 9.1 admite sin forzarla la posibilidad de que el médico comunique los datos a un tercero sin el consentimiento del paciente cuando concurren razones suficientes (riesgo grave). Ello por cuanto el derecho a no saber no es un derecho absoluto y no conlleva de ninguna manera el derecho a que los demás tampoco sepan. Así lo ha dispuesto, como veremos en el apartado 3.10 de este trabajo, la Ley de Investigación Biomédica (LIB) respecto del derecho a no saber los datos genéticos obtenidos de un test genético.

En fin, del segundo inciso del artículo comentado se desprende que debe respetarse la voluntad del paciente de no saber, pero, en línea con las previsiones de la LIB, consideramos que el primer inciso establece como contrapartida a este derecho a no saber la posibilidad de que el profesional sanitario comunique esa información a terceros cuando el paciente tuviera una enfermedad infecciosa o de otro orden que suponga un riesgo grave para la salud de los mismos[180]. En cualquier caso, además de la habilitación *ex lege* que defendemos, la comunicación de los datos a terceros quedaría amparada por la eximente de estado de necesidad.

[179] Véase ARCOS VIEIRA, M.ª L., "Consentimiento no informado: reflexiones en torno a la existencia de un "Derecho a no saber" aplicado a la información clínica.", en *Autonomía del paciente e intereses de terceros: límites,* Thomson-Reuters-ARANZADI, 2016, p. 62.

[180] Véase en este sentido GÓMEZ SÁNCHEZ, Y., voz "Derecho a no saber" en ROMEO CASABONA (director) *Enciclopedia de Bioderecho y Bioética,* Comares S.L., 2011, Tomo I, pp. 597-598.

Esta circunstancia ocurre con relativa frecuencia en la relación clínica que se entabla entre el profesional sanitario y pacientes con determinadas dolencias, ejerzan o no su derecho a no saber: enfermos mentales, pacientes con episodios depresivos agudos, portadores de enfermedades infecciosas (seropositivos, etc.), o a los que se realizan determinadas pruebas biológicas, etc. Por lo que le manifiesta el propio paciente o por su actitud, el médico tiene fundadas sospechas de que pretende causar un daño serio a otra u otras personas, o le es indiferente el daño grave que pueda causar por no informarles debidamente. El médico tiene el deber ético y legal de evitar el daño arrinconando, si es preciso, su deber de secreto[181].

Un caso particular es el de las personas que padecen la infección de VIH/SIDA. La estigmatización social que conlleva esta enfermedad y los graves perjuicios que su conocimiento por terceros acarrea a las personas que la padecen, ha impulsado a algunos autores a dar prioridad al deber de secreto sobre la información a un tercero para salvaguardar su salud, si bien la mayoría de la doctrina afirma que debe darse prioridad a la salud de terceros frente a la intimidad del seroportador[182].

En relación a la propuesta contenida en el apartado 1.a) esto es, la revelación del secreto cuando el paciente pertenezca a profesiones que implican riesgos colectivos y, en razón de la relación clínica con el mismo, tenga razones fundadas de que pueda provocar inminentemente una catástrofe, resulta oportuno hacer referencia al documento de posición colegial "*EL SECRETO PROFESIONAL MÉDICO Y LA PROTECCIÓN A TERCEROS. Reflexiones y propuestas a raíz del accidente de aviación de Germanwings ocurrido en los Alpes franceses el 24 de marzo de 2015*", elaborado por el Colegio de Médicos de Barcelona[183], en el que se razona al respecto lo siguiente:

> "Como vemos, los límites legales y deontológicos del secreto profesional quedan vinculados, en nuestro país, a una previsión legal y a la certeza de un riesgo o peligro para el mismo profesional, para el paciente o para terceros.
>
> En el ámbito laboral, estos límites se encontrarían en la salud de los trabajadores o de terceros, o en determinados sectores, en la protección frente a riesgos específicos y actividades de especial peligrosidad. Así, ante supuestos de enfermedad que pudieran poner en riesgo el trabajador, o la salud o vida de terceros, consecuencia de su actuación

[181] Esta problemática se da particularmente en el ámbito de la asistencia psiquiátrica. Es famoso el caso Tarasoff, por ser uno de los más representativos del secreto médico en psiquiatría, en el que la Corte Suprema de California terminó sentenciando en 1974 que cuando un paciente representa un peligro para terceros, hay que tomar las medidas necesarias para proteger a la posible víctima, las cuales pueden ir **desde informar a la persona en riesgo**, notificarlo a la policía, o lo tal vez más acertado, plantear un ingreso involuntario de carácter urgente. Véase sobre este caso y otros similares BARBERO GUTIÉRREZ, J., SÁNCHEZ CABALLERO, M. y CORTECERO, J. M., "Secreto profesional y riesgo vital para un tercero identificado: metodología de análisis ético en torno a un caso" en *Revista de la Asociación Española de Neuropsiquiatría,* vol. 33, núm. 119, 2013, pp. 555-573.

[182] Véase al respecto, SÚAREZ RUBIO, S., *Constitución y privacidad sanitaria,* Tirant lo Blanch. 2015, pp. 242-245.

[183] Col·legi de Metges de Barcelona. "El secreto profesional médico y la protección a terceros. Reflexiones y propuestas a raíz del accidente de aviación de Germanwings ocurrido en los Alpes franceses el 24 de marzo de 2015". Documento de posición colegial.
Disponible en: http://www.asociaciongwi9525.org/doc/sec%20i%20proc%20a%20tercers.pdf

profesional, encontramos como norma habilitante para el levantamiento del secreto de forma proporcionada el artículo 22 de la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales, en virtud del cual el médico podrá informar al empresario de las conclusiones que se deriven de los reconocimientos efectuados a los trabajadores, en relación con su aptitud para desarrollar el trabajo. La comunicación no se hará respecto al diagnóstico del trabajador, sino respecto a su falta de aptitud para desarrollar su trabajo habitual.

El problema se plantea cuando esta circunstancia no es conocida por los servicios de salud laboral de la empresa y sí, en cambio, por el médico del sistema público de salud —que prescribirá la baja laboral tras el oportuno reconocimiento—, o por el médico asistencial de ámbito privado.

Nuestro ordenamiento jurídico prevé que el médico del sistema público entregará al trabajador dos copias de la baja médica, una para el interesado y la otra para la empresa, y corresponderá al trabajador la entrega a la empresa del correspondiente parte médico de baja.

Por lo tanto, si el trabajador no entrega esta información a la empresa, y continúa trabajando, esta puede desconocer esta situación de incapacidad temporal, a pesar de que pueda ser tributaria de un riesgo cierto para la propia vida o salud del trabajador o para la de terceros.

Esta regulación actual seguramente responde y pivota en la relación médico-paciente y en la confianza mutua que fundamenta esta relación, pero el engaño por parte de un paciente no es siempre evitable, sino que es posible, y no podemos exigir a los médicos que se conviertan en inspectores de control de los pacientes.

En este sentido, y como ya se sugiere en otros apartados de este documento, para evitar que la decisión de comunicar a la empresa la incapacidad temporal para desarrollar sus tareas quede en manos del trabajador, sería razonable y conveniente promover una reforma de la normativa actual que, haciendo uso de las TIC, como ya se prevé en la actual regulación de esta y otras materias, se determinara una comunicación automática de la baja laboral en la empresa a través de la Seguridad Social. Obviamente, el alta del proceso de incapacidad laboral debería conllevar el mismo automatismo de comunicación.

En cambio, la situación en determinados supuestos podría ser más compleja en el ámbito asistencial de la medicina privada, dado que el médico no dispone del mecanismo de la baja laboral que, aunque no es definitivo, ayuda en este proceso de comunicación de la baja.

En este aspecto, hay que partir del hecho de que el médico de cualquier ámbito asistencial es la persona competente para emitir el diagnóstico y el pronóstico de la enfermedad en base a su juicio clínico, y en este proceso, si detecta un riesgo para el mismo paciente o para terceros —y en este caso, que pueda adquirir especial relevancia en atención a su profesión—, debería ser proactivo de forma discreta, moderada, ponderada y proporcionada, y comunicar esa circunstancia solo a quien corresponda para evitar el eventual daño que se pueda derivar de ese riesgo detectado, y ello amparado en las normas del Código de Deontología y en la doctrina constitucional, antes mencionadas.

En los supuestos de extrema gravedad, nuestro ordenamiento jurídico ya prevé mecanismos de emergencia que puedan dar respuesta, como el ingreso involuntario urgente, con el posterior control judicial. Pero en aquellos supuestos en que la situación no se haga tan evidente y no sea necesariamente tributaria de ingreso, y en cambio requiera de una actuación proactiva por parte del médico, habría que plantearse dotar al

profesional sanitario del mecanismo y de los medios que pudieran hacer más fluida la comunicación, sobre todo cuando el médico pertenece al ámbito asistencial privado."

En definitiva, el deber de confidencialidad/secreto puede ceder ante situaciones en las que hay un interés prevalente al de mantener el sigilo respecto de determinada información.[184] La jurisprudencia[185] ha establecido los siguientes requisitos que justificarían la injerencia en la intimidad:

a) Existencia de una finalidad constitucionalmente legítima (como son la protección de la salud, la vida o la integridad física).

b) Previsión legal de la medida limitativa.

c) Observancia de la proporcionalidad de la medida, que requerirá: un juicio de idoneidad (para valorar si la medida es susceptible de conseguir la finalidad perseguida); un juicio de necesidad (para valorar que no existe otra medida más moderada para la consecución de la finalidad, y que sea igualmente eficaz), y el juicio de proporcionalidad en sentido estricto (que requerirá la valoración sobre si la medida es ponderada y sobre si se derivan más beneficios para el interés general que perjuicios por encima de valores en conflicto).

Los comités de ética asistenciales y, en su caso, los colegios profesionales, deben ser órganos abiertos y proclives a facilitar un rápido asesoramiento al profesional sanitario respecto de esta cuestión ayudando a realizar un juicio de proporcionalidad adecuado conforme a las premisas exigidas jurisprudencialmente.

La comunicación de datos a terceras personas amparada en la eximente de estado de necesidad tiene, a su vez, sus límites. Así, por ejemplo, se viene negando al personal auxiliar que trabaja en hospitales y puede entrar en contacto con fluidos y productos

[184] De todos modos, por algunos se postula el reconocimiento expreso de un secreto privilegiado en psiquiatría, en ningún caso derogable, a favor de las confidencias entre psiquiatra y paciente. Así, HERRANZ RODRÍGUEZ, G, manifiesta al respecto que "Se expande, en los estatutos legales, el campo de derogaciones del secreto, evolución aceptable si tal sacrificio de la intimidad de la relación médico-paciente está al servicio de los pocos derechos y bienes humanos que le son superiores: denuncia de la intención de dañar a terceros, de los no idóneos, a causa de enfermedad, para conducir autos o aeroplanos o para tener armas, de los sospechosos de abuso de niños o desvalidos, del colega que abusa sexualmente de sus pacientes. Pero, en ocasiones se pide al médico que revele información sensible que no parece estar al servicio de una causa superior, sino de la mera eficiencia administrativa o judicial. El médico podrá, por razones deontológicas, oponerse a tales exigencias. Sería de desear que no tarde en llegar la regulación legal del secreto profesional del médico, que especificase los delitos y las penas amenazadas contra quien falte a este deber tan humano de respetar la intimidad de otro. Sería también muy interesante que esa normativa concediera el reconocimiento de secreto privilegiado, nunca derogable, a las confidencias entre psiquiatra y paciente, cuya intimidad no cede a otras que, como la comunicación entre confesor y penitente, entre marido y mujer, o entre abogado y cliente, gozan ya en muchas partes de ese privilegio especial. La Corte Suprema de los Estados Unidos acaba de hacerlo así.", en *La ética médica y sus relaciones con la historia clínica y el secreto*, ponencia del III Congreso Nacional de Derecho Sanitario, 1996, disponible en: http://www.aeds.org/congreso/congresos-aeds/congreso3_13.php

[185] Sentencia del Tribunal Constitucional 37/1998, de 17 de febrero, y Sentencia del Tribunal Supremo de 19 de abril de 2011, f. j. sexto -RJ/2011/2309-, entre otras.

biológicos contaminantes, el derecho a conocer qué pacientes de los que atienden tienen una enfermedad infectocontagiosa como la hepatitis o el sida. ¿No sería aplicable aquí la eximente de estado de necesidad? No, por cuanto se entiende que el deber de secreto prevalece en estos casos ya que la protección de los trabajadores que atienden a personas internadas en hospitales pasa por la aplicación de las medidas de protección universal debidamente protocolizadas, que deben ser aplicadas siempre, independientemente de que se conozca o no la patología que presenta el paciente. Por su parte, la jurisprudencia no admite la eximente de estado de necesidad para salvar bienes privativos (salud, economía personal o familiar) si se atenta contra bienes colectivos cuya titularidad ostenta la sociedad o el estado -por ejemplo, salud pública-, por considerar que tienen un valor superior (entre otras muchas, STS 340/2005, de 8 de marzo).

3.6. Expedición de certificados de nacimiento y de defunción[186].

Propuesta de regulación:

El facultativo que haya asistido al difunto en su última enfermedad o cualquier otro que reconozca el cadáver enviará inmediatamente al Registro Civil el certificado de defunción En el certificado de defunción deben constar los datos de identificación del médico, del paciente y la hora de la muerte. No deberán figurar las causas inmediata y fundamental de la muerte.

---

[186] Ley 20/2011, de 21 de julio, del Registro Civil:
Artículo 45. *Obligados a promover la inscripción de nacimiento.*
Están obligados a promover la inscripción de nacimiento:
La dirección de hospitales, clínicas y establecimientos sanitarios.
El personal médico o sanitario que haya atendido el parto, cuando éste haya tenido lugar fuera de establecimiento sanitario.
Artículo 63. *Obligados a promover la inscripción de fallecimiento.*
Están obligados a promover la inscripción de fallecimiento:
La dirección de hospitales, clínicas y establecimientos sanitarios donde se produzca el fallecimiento.
El personal médico que certifica el fallecimiento, cuando éste haya tenido lugar fuera del establecimiento sanitario.
Artículo 64 *Comunicación de la defunción por los centros sanitarios*
La dirección de hospitales, clínicas y establecimientos sanitarios comunicará a la Oficina del Registro Civil competente y al Instituto Nacional de Estadística cada uno de los fallecimientos que hayan tenido lugar en su centro sanitario. La comunicación se remitirá por medios electrónicos en el plazo que se establezca reglamentariamente mediante el envío del formulario oficial debidamente cumplimentado, acompañado del certificado médico firmado por el facultativo. Dicha remisión será realizada por personal del centro sanitario, que usará para ello mecanismos seguros de identificación y firma electrónicos.
Artículo 66 *Certificado médico de defunción*
En ningún caso podrá efectuarse la inscripción de defunción sin que se haya presentado ante el Registro Civil el certificado médico de defunción. En el certificado, además de las circunstancias necesarias para la práctica de la inscripción, deberán recogerse aquellas que se precisen a los fines del Instituto Nacional de Estadística y, en todo caso, la existencia o no de indicios de muerte violenta y, en su caso, la incoación o no de diligencias judiciales por el fallecimiento si le fueran conocidas o cualquier motivo por el que, a juicio del facultativo, no deba expedirse la licencia de enterramiento.
Las circunstancias mencionadas en el segundo inciso del párrafo anterior no serán incorporadas a la inscripción de defunción ni serán objeto del régimen de publicidad establecido en esta Ley, siendo su única finalidad la establecida en este artículo.

En el certificado, además de las circunstancias reseñadas en el párrafo anterior para la práctica de la inscripción, deberán recogerse aquellas que se precisen a los fines del Instituto Nacional de Estadística y, en todo caso, la existencia o no de indicios de muerte violenta y, en su caso, la incoación o no de diligencias judiciales por el fallecimiento si le fueran conocidas, o cualquier motivo por el que, a juicio del facultativo, no deba expedirse la licencia de enterramiento. Estas circunstancias no serán incorporadas a la inscripción de defunción ni serán objeto del régimen de publicidad establecido en la Ley del Registro Civil.

Comentario exegético:

Los certificados de nacimiento no presentan problemas particulares dignos de mención.

Respecto de los certificados médicos de defunción se ha escrito[187] lo siguiente: "Son ya clásicas las reticencias de los médicos a firmar los Certificados Médicos de Defunción. En ocasiones subyace el temor de que se le pase por alto un homicidio. Con frecuencia alegan, como motivo, que no conocen al paciente y que esta labor compete exclusivamente al médico de cabecera. Sin embargo, el Reglamento del Registro Civil dice textualmente en su artículo 274 que "el facultativo que haya asistido al difunto en su última enfermedad o cualquier otro que reconozca el cadáver enviará inmediatamente al Registro el parte de defunción." Por tanto, aun siendo reiterativos, vale la pena insistir en que, según este precepto, el CMD no tiene por qué firmarlo el médico que mejor conoce la historia clínica del paciente. Ni tan siquiera aquel que lo atendió en la enfermedad que le produjo la muerte, sino que puede hacerlo cualquier médico que tenga la posibilidad de explorar el cadáver. La Declaración realizada por la Organización Médica Colegial sobre las peculiaridades del certificado médico de defunción recomienda que dicho documento ha de extenderlo el médico que asistió al paciente durante el proceso que le condujo a la muerte, o el que estuvo presente en los últimos momentos, o el que lo atendió en su última enfermedad. Solo en último caso, podrá redactarlo cualquier otro médico que haya reconocido el cadáver y pueda reconstruir fiablemente los mecanismos de muerte."

En cualquier caso, haciendo abstracción de la bondad o no de esta obligación que se impone a los médicos, recojo aquí los requisitos incorporados por el apartado siete del artículo segundo de la Ley 19/2015, de 13 de julio, de medidas de reforma administrativa en el ámbito de la administración de justicia y del Registro Civil.

Respecto de los problemas de confidencialidad que suscitan los certificados médicos de defunción, reseñar que en otros países de nuestro entorno europeo se tiene más presente esta cuestión, de manera que se obliga a certificar la defunción, pero no sus causas, esto es, no es preceptivo que conste el diagnóstico de las causas de la muerte. Causas como el suicidio y otras exigen preservar al máximo la confidencialidad de la información que

[187] BUGARÍN GONZÁLEZ, R, SEOANE DÍAZ B. "El certificado médico de defunción." en *Galicia Clínica*, 2014; 75 (1), pp. 12-16.

se puede conocer por terceros a través del certificado de defunción. Así se evita el acceso a los datos clínicos de las personas que intervienen en el periodo posterior al fallecimiento. De ahí que nuestra propuesta normativa exima de la obligación de hacer constar el diagnóstico de la causa de la muerte. El diagnóstico de la causa de la muerte deberá registrase por otra vía que garantice la confidencialidad e intimidad de la persona fallecida.

3.7. Acceso a la historia clínica con fines judiciales[188].

Propuesta de regulación:

1. El acceso a la historia clínica con fines judiciales[189] *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.*

2. 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 procederá a lo que dispongan los jueces y tribunales en el proceso correspondiente.

3. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso, de manera que solo se facilitarán los documentos o datos relacionados con el proceso asistencial afectado que deberá especificarse claramente en la petición judicial.[190]

4. La cesión de la historia clínica o de determinados datos de la misma a los jueces y tribunales deberá hacerse exclusivamente en soporte informático y con las suficientes garantías para que nos sea accesible indebidamente por terceros. A tales efectos, se establecerán los procedimientos protocolizados necesarios.

Comentario exegético:

En lo que hace a la entrega de la historia clínica, de entrada, señalar que el artículo 118 CE establece que es obligada la plena colaboración de las Administraciones sanitarias con la administración de justicia en el curso del proceso. En los procesos judiciales por responsabilidad médica, tanto contencioso-administrativos como civiles o penales, la historia clínica es un elemento clave para dilucidar la existencia o no de

[188] Artículo 16.3 Ley 41/2002, de 14 de noviembre, básica de autonomía del paciente.

[189] El artículo 256.1.5 bis) de la LECivil alude expresamente a la historia clínica: «*Todo juicio podrá prepararse… por la petición de la historia clínica al Centro sanitario o profesional que la custodie, en las condiciones y con el contenido que establece la Ley*».

[190] El Auto del Juzgado de Primera Instancia núm. 6 de Pamplona, de 20 de octubre de 2006, señala que "la confidencialidad de los datos que integran la historia clínica y el derecho a la prueba en el proceso obligan a delimitar cuidadosamente la parte del historial que guarda relación directa con lo discutido en el juicio, de modo que la petición genérica de prueba es inadmisible."

responsabilidad[191]. Como apunta SARRATO MARTÍNEZ[192] "la historia clínica ante los Tribunales tiene un extraordinario valor probatorio. Constituye uno de los mejores instrumentos de defensa en juicio del médico diligente, pero también sirve para proteger al enfermo cuando la asistencia prestada no ha sido correcta. Un procedimiento judicial puede tener por objeto averiguar si el personal sanitario, a consecuencia de su actuación profesional, ha incidido en responsabilidad contractual o extracontractual por el incumplimiento de la «lex artis ad hoc» (proceso civil), si dicho personal ha cometido un delito o falta (proceso penal) o si existe responsabilidad patrimonial de la Administración por el funcionamiento normal o anormal de los servicios sanitarios (proceso contencioso-administrativo). La historia clínica también puede ser requerida para su aportación en un proceso de naturaleza laboral o de Seguridad Social."

En el Decálogo de la Historia Clínica aprobado en marzo de 2017 por la Organización Médica Colegial, se dice:

> 7. La historia clínica como medio de prueba. El uso judicial de la historia clínica en el ámbito civil requiere la previa autorización del paciente. En el ámbito penal, cuando la historia se convierte en elemento de prueba de un posible delito, se debe entregar; por parte del médico o del centro, la precaución deontológica estará en informar al juez de la existencia en la misma de datos sensibles que si son irrelevantes para la causa investigada, se podrían segregar del total del documento, manteniéndose protegidos. Una vez que la historia se halla en posesión del Juez, será éste el garante de su custodia y preservación de la confidencialidad de los datos contenidos en la misma.

No obstante, es criterio doctrinal generalizado que cuando es el juez el que de oficio requiere la entrega de la historia clínica, el artículo 16.3 LBAP obliga a entender que el centro público o el médico privado, están obligados a su entrega en todo caso, tanto se trate de un proceso penal, civil o contencioso-administrativo.

La historia clínica no tiene consideración de documento público a efectos probatorios, por lo que admite prueba en contrario, aunque penalmente tiene la condición de documento oficial (art. 390 CP). El contenido de la historia clínica lo decide el médico, no el paciente (art. 15.2 y 3 LBAP) y debe ser inteligible, asumiendo el médico en caso contrario la obligación de aclarar su contenido en el juicio -STS de 26 de marzo de 2001. El órgano judicial debe precisar qué parte o partes de la historia clínica precisa. Podrán incluir las anotaciones subjetivas, si bien, en este caso, el médico le advertirá de este carácter a fin de que valore su trascendencia[193].

---

[191] Véase GUTIÉRREZ BARRENENGOA, A., "La historia clínica como prueba en el Proceso Judicial por responsabilidad médica" en el libro colectivo *Responsabilidad médica civil y penal por presunta mala práctica profesional,* Editorial Dykinson, 2012, pp. 323-334.

[192] "El régimen legal de acceso a la historia clínica y sus garantías" en *Revista Jurídica de Castilla y León*, núm. 17, 2009, p. 200.

[193] Sobre esta temática véase LARIOS RISCO, D., en *Guía Práctica de Derechos de los Pacientes y de los Profesionales sanitarios,* Thomson-Reuters ARANZADI, 2016, pp. 165 a 195.

Es frecuente que, a pesar de estar la historia clínica digitalizada, se remita la información al juez en formato papel lo que posibilita (de hecho, así suele ocurrir) el acceso a los datos de muchas personas distintas al juez, por lo que es del todo recomendable que la remisión se haga por vía electrónica y con suficientes garantías para preservar la confidencialidad de los datos remitidos[194].

En cualquier caso, la remisión de la historia clínica a petición de un juez o tribunal está necesitada de una regulación más actual y detallada. Al respecto, LACHICA LÓPEZ[195], profesora titular de medicina legal, afirmaba en el año 2001 que "Pese a que el derecho de la autoridad judicial a acceder a la información y documentación clínica nunca se discute, debería ser objeto de una regulación más actual y acorde con los intereses del conflicto, dado que nuestras leyes de enjuiciamiento civil y criminal se publicaron en un contexto muy diferente del actual. Así, por ejemplo, la naturaleza de la información clínica que puede necesitar un Juzgado o Tribunal para resolver un procedimiento judicial estará en función de la acción que se ejercite: una reclamación por responsabilidad civil del médico por mala praxis, una acción de reclamación por mal funcionamiento del servicio de salud, un procedimiento para declarar la incapacidad laboral de un trabajador, etc. Por ello, cuando las autoridades judiciales demandan la entrega de la historia clínica de un paciente para incorporarla, en bloque, a un procedimiento judicial, el médico tendrá derecho a exigir que se precise qué informes o datos de la misma se consideran necesarios por la autoridad judicial para el buen fin de la investigación. Así, por ejemplo, en Estados Unidos la American Medical Association insiste en la necesidad de determinar qué parte de historia o de información se precisa, de qué periodo de tiempo y el fin para el que se solicita.". Desafortunadamente, esta regulación no se ha producido todavía.

Finalmente, en lo que hace a las resoluciones judiciales que ponen fin al proceso, la LOPJ, su artículo 235 dispone que:

> El acceso al texto de las sentencias, o a determinados extremos de las mismas, o a otras resoluciones dictadas en el seno del proceso, solo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.

Y su artículo 236 quinquies establece que:

> Los jueces y tribunales, y los letrados de la administración de justicia conforme a sus competencias procesales, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar su

[194] En este sentido, MILLÁN CALANTI, R., Historia electrónica: accesos compatibles", en PALOMAR OLMEDA, A. y CANTERO MARTÍNEZ, J. (dirección) *Tratado de Derecho Sanitario,* Tomo I, Thomson-Reuters-ARANZADI, 2013, p. 796.

[195] "El secreto médico y el consentimiento informado en los informes periciales" en *Cuadernos de Medicina Forense*, núm. 22, 2002.

> derecho a la tutela judicial efectiva. Del mismo modo procederán respecto del acceso por las partes a los datos personales que pudieran contener las sentencias y demás resoluciones dictadas en el seno del proceso, sin perjuicio de la aplicación en los demás supuestos de lo establecido en el artículo 235 bis[196].

Comprobamos, pues, que en las resoluciones y sentencias se procede a la disociación de datos personales[197] y que los jueces y demás personal judicial intervinientes en los procesos judiciales quedan sujetos al deber de secreto.

3.8. Vigilancia de la salud de los trabajadores.

Propuesta de regulación:

1. Los profesionales sanitarios responsables de la vigilancia de la salud de los trabajadores deben facilitar la información médica obtenida en los reconocimientos médicos de los trabajadores a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, así como las conclusiones derivadas de los reconocimientos al empresario y a las personas u órganos con responsabilidades en materia de prevención, en los términos establecidos en el artículo 22.4 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

2. El médico podrá comunicar al empresario la situación de incapacidad transitoria de un trabajador cuando estime existe peligro serio de que este pueda exponer a determinados riesgos a terceros por no haber comunicado su situación de incapacidad transitoria al empresario.

Comentario exegético:

Como señala GOMEZ RIVERO[198], la genuina razón de ser de los reconocimientos laborales no se enfoca directamente a la persona en cuanto posible enfermo, sino en su calidad de trabajador, bien sea para evaluar los riesgos que pueda sufrir en el puesto de trabajo y adoptar las medidas de protección, bien para evitar riesgos colectivos[199]. En palabras de esta autora, tienen vocación de "exteriorización".

---

[196] Los artículos citados de la Ley Orgánica del Poder Judicial fueron introducidos por la L.O. 7/2015, de 21 de julio.

[197] La disociación consiste en poner solo los nombres de los litigantes, sin apellidos, pero, combinando el nombre con los demás datos y circunstancias que se describen en las sentencias y resoluciones judiciales, resulta extremadamente fácil identificar a las personas litigantes y, en consecuencia, anudar los datos de salud extraídos de las historias clínicas a dichas personas.

[198] Voz "Secreto médico", en ROMEO CASABONA, C. (director) *Enciclopedia de Bioderecho y Bioética,* Comares S.L., Tomo I, 2011, p. 1512.

[199] Sobre los reconocimientos médicos en el ámbito laboral véase GOÑI SEIN, J. L. y RODRÍGUEZ SANZ DE GALDEANO, B., "El reconocimiento médico de aptitud profesional del aspirante al empleo.", en el libro colectivo ALENZA GARCÍA, J. F. y ARCOS VIEIRA M.ª L. (directores) *Nuevas Perspectivas Jurídico-Éticas en Derecho Sanitario,* Thomson Reuters ARANZADI, 2013, pp. 301-336.

El artículo 22 de la Ley de Prevención de Riesgos Laborales, contempla tres ámbitos de revelación de los datos obtenidos de un reconocimiento médico laboral: a) al propio trabajador; b) a las autoridades sanitarias que llevan a cabo la vigilancia de la salud de los trabajadores[200]; c) al empresario y a los órganos con responsabilidad en materia de prevención laboral (delegados de prevención, miembros del comité de seguridad y salud laboral o de los servicios de prevención) respecto de las conclusiones derivadas del reconocimiento. Al empresario y órganos de prevención solo han de comunicarse los aspectos conclusivos que les interesen para tomar las medidas oportunas, pero sin poder acceder a los datos propiamente médicos, pero, como bien advierte esta autora[201], no puede desconocerse la dificultad para desligar lo que sean meras conclusiones acerca del estado de salud respecto a la enfermedad que la motiva. Además, GOÑI SEIN[202] también advierte que es posible que el empresario deba acceder de modo específico a información personal del trabajador necesaria para el cumplimiento de sus obligaciones que desborden el contenido apto/no apto, y que en tales casos la legitimación derivaría de la propia ley, aunque se limitará a los datos estrictamente necesarios. Así pues, además de a las autoridades sanitarias, también se informa, aunque limitadamente, al empresario y a órganos de esa empresa encargados de la prevención. De ahí que no considero oportuno incluir este supuesto en el ámbito del secreto médico compartido y lo incluyo en las excepciones al deber de secreto.

En otro orden de cosas, señalar que el Colegio de Médicos de Barcelona, en el informe "EL SECRETO PROFESIONAL MÉDICO Y LA PROTECCIÓN A TERCEROS. Reflexiones y propuestas a raíz del accidente de aviación de Germanwings ocurrido en los Alpes franceses el 24 de marzo de 2015"[203], al que ya he hecho referencia, aboga por establecer un marco normativo que facilite canales de comunicación estables entre la medicina asistencial (tanto pública como privada) y la medicina de empresa, con un procedimiento que supuestamente no implicaría la vulneración del deber de secreto por parte del médico, mientras que aportaría ventajas desde el punto de vista organizativo y de garantía de la seguridad. Actualmente, las situaciones de incapacidad transitorias las comunica directamente el trabajador.

3.9. Asistencia a menores de edad maduros y deber de secreto.

---

[200] El Informe Jurídico 206/2010 de la Agencia Española de Protección de Datos, ratifica la transmisión a las autoridades sanitarias afirmando que "se prohíbe la transmisión de la información médica obtenida al amparo de lo dispuesto en la Ley de Prevención de Riesgos Laborales a cualquier tercero distinto del personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de salud de los trabajadores (…) por lo que cualquier otra cesión a otros profesionales o centros médicos que se realice por el servicio de prevención ajeno con la finalidad de vigilancia de salud, requerirá el consentimiento expreso de los afectados."

[201] Ibidem, p. 1513.

[202] "El tratamiento de datos de salud del trabajador" en el libro colectivo ARCOS VIEIRA, Mª L. (directora) *Autonomía del paciente e intereses de terceros: límites,* Thomson Reuters ARANZADI, 2016, p. 229.

[203] disponible en: file:///C:/Users/piluc/Desktop/Trabajos%20Juan%20Luis/secreto%20médico%20y%20proteción%20de%20terceros%202016.pdf

El artículo 9.4 de la LBAP, redactado por la disposición final segunda de la Ley 26/2015, de 28 de julio, establece que

> Cuando se trate de menores emancipados o mayores de 16 años que no se encuentren en los supuestos b) y c) del apartado anterior, no cabe prestar el consentimiento por representación. No obstante lo dispuesto en el párrafo anterior, cuando se trate de una actuación de grave riesgo para la vida o salud del menor, según el criterio del facultativo, el consentimiento lo prestará el representante legal del menor, una vez oída y tenida en cuenta la opinión del mismo.

A su vez, el artículo 9.5, también redactado por la disposición final segunda de la Ley 26/2015, establece que

> Para la interrupción voluntaria del embarazo de menores de edad o personas con capacidad modificada judicialmente será preciso, además de su manifestación de voluntad, el consentimiento expreso de sus representantes legales.

Así pues, en la medida en que la ley, en las circunstancias descritas, obliga a los médicos, aun a pesar de la oposición de los menores, a comunicar a sus padres o representantes legales sus datos de salud a efectos de obtener su consentimiento para realizar la actuación pretendida, estamos ante supuestos de exoneración del deber de secreto por imperativo legal.

Esta modificación de la LBAP ha sido criticada por la generalidad de la doctrina[204]. Y, en efecto, la restrictiva visión de la capacidad para decidir del menor maduro que subyace en estas determinaciones legales no armoniza con la teleología de la LBAP y de las leyes sobre protección jurídica de la infancia y de los menores de edad, ni con la doctrina que mantiene el Tribunal Constitucional, entre otras, en sus sentencias 154/2002, de 18 de julio y 37/2011, de 28 de marzo, en cuanto se ha retrocedido a posiciones excesivamente paternalistas que se compadecen muy mal con las reales capacidades de los menores de edad maduros. Pero, en fin, la restrictiva capacidad que estos nuevos apartados del artículo 9 atribuyen al menor maduro con 16 años o a la menor de edad que desea abortar, es cuestión que no nos compete abordar ahora, por lo que basta aquí con constatar, sin más, estos casos en los que el legislador impone a los facultativos el deber de comunicar datos de salud a terceras personas distintas al interesado para poder efectuar una intervención clínica, por lo que implícitamente les releva de su deber de secreto profesional.

---

[204] BELTRÁN AGUIRRE, J. L. "Los derechos de los menores de edad en el ámbito sanitario" en PALOMAR OLMEDA, A. y CANTERO MARTÍNEZ, J. (dirección), *Tratado de Derecho Sanitario*, Tomo I, Thomson Reuters Aranzadi, 2013, pp. 873-875; ABELLÁN, F, "La autonomía del menor ante situaciones de riesgo grave" en Diario Médico de 17 de octubre de 22012; DE MONTALVO, F. "Diez años de regulación del menor maduro" en Diario Médico de 10 de diciembre de 2012; Reportaje del Diario Médico de 21 de octubre de 2015 donde se recogen la opinión de diversas personas y entidades criticando la reforma por excesivamente paternalista (Asociación Española de Pediatría, ESQUERDA, M., directora del Instituto Borja de Bioética, CARLOS SARDINERO, etc.); LOMAS HERNÁNDEZ, V. Boletín de Derecho Sanitario y Bioética (SESCAM), núm. 126, de julio-agosto de 2015, pp. 29-30; etc. No obstante, también pueden encontrarse algunos trabajos en los que no se critica en absoluto la reforma. Así, la Fiscal General del Estado MADRIGAL MARTÍNEZ-PEREDA, C. "Menores y tratamientos médicos" en *Derecho y Salud,* vol. 26, Extraordinario XXV Congreso 2016, pp. 12-21.

Por lo dicho, no incorporamos aquí una propuesta de regulación ya que, en nuestro criterio, lo que lo que procedería es que se deroguen los apartados 4 y 5 del artículo 9 de la LBAP mediante una disposición adicional de la futura ley que regule el secreto profesional.

3.10. Por habilitación *ex lege*: derecho a no conocer datos genéticos u otros de carácter personal obtenidos en el curso de una investigación biomédica o de un análisis muestras biológicas *vs* grave riesgo para familiares biológicos.

Propuesta de regulación:

Ante la renuncia del sujeto a conocer la información genética obtenida de un análisis genético u otra de carácter personal obtenidos en el curso de una investigación biomédica o de un análisis de muestras biológicas por otros motivos, cuando, según criterio del médico responsable, sea necesaria para evitar un grave perjuicio para la salud de sus familiares biológicos, se podrá informar a un familiar próximo o a un representante, previa consulta del correspondiente comité de ética asistencial. En todo caso, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades.

Comentario exegético:

Un ámbito en el que es frecuente la colisión de derechos es el de los datos genéticos. Son, por ejemplo, los casos de determinación de la maternidad o paternidad, o la realización por una persona de un test genético del que resulta una predisposición familiar a padecer una determinada enfermedad. Otro ámbito es el de personas portadoras de enfermedades infecciosas. Y no es lo mismo acceder al dato genético para que un hijo pueda conocer la identidad de su madre, o para conocer la prevalencia familiar a padecer una determinada enfermedad, o para cobrar una póliza de seguro, o para acceder a un puesto de trabajo. Por ello, en la abundante casuística que puede presentarse, siempre hay que hacer una ponderación de los intereses enfrentados, particulares o públicos. La aplicación del principio de proporcionalidad es esencial en esa ponderación.

Relata GÓMEZ RIVERO[205] que la doctrina norteamericana y australiana, partiendo del hecho de que el dato genético es común a otros familiares, defiende que ese dato pierda como referente de su titularidad a la persona individual sobre la que se ha practicado el análisis para obtener el dato genético, para pasar a adquirir una titularidad familiar, lo que, sin más, posibilitaría la comunicación de los datos a la familia biológica. A pesar de la razonabilidad de esta posición doctrinal, no es así como se ha tratado el tema en nuestro ordenamiento jurídico. De entrada, revelar el dato genético a un familiar sin el consentimiento del afectado, entraría en la lógica de la eximente de estado de

[205] GÓMEZ RIVERO, C., voz "Secreto profesional" en ROMEO CASABONA, C. M.ª (director) en *Enciclopedia de Bioderecho y Bioética,* Tomo II, Editorial Comares S. L., 2011, pp. 1510-1511.

necesidad[206], pero, como apunta esta autora, le faltarían dos requisitos imprescindibles para instrumentarlo por este cauce: no hay un riesgo inminente y tampoco un riesgo futuro cierto. De ahí que nuestro legislador haya optado por habilitar *ex lege* al profesional sanitario a revelar el secreto profesional. En efecto, La LIB (artículos 4.5 y 49.2[207]), sancionan el derecho a no saber y, en consecuencia, la imposibilidad de que el sujeto fuente, al no conocerla, transmita a terceros información que pueda resultar de interés para ellos, pero como contrapartida a este derecho a no saber prevé expresamente la posibilidad de que el profesional sanitario comunique los datos genéticos a familiares cuando tuviera una condición transmisible (por ejemplo, a la descendencia) que suponga un riesgo grave para la salud de los mismos, o exista una predisposición familiar a padecer una determinada enfermedad.[208] Por su parte, el Código de Deontología Médica autoriza a revelar el secreto "*si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo*" (artículo 30.1.c).

La LBAP no contempla expresamente este supuesto a efectos de exonerar al profesional sanitario de su deber de secreto cuando tratan las excepciones al requisito de previo consentimiento del interesado. Sí contempla implícitamente esta realidad. En efecto, su artículo 9.1 establece que "La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso." Así pues, este precepto sanciona el derecho a no saber, que consiste básicamente en el reconocimiento de la voluntad de un sujeto de no ser informado sobre aspectos que afectan a su salud[209], y, en consecuencia, la imposibilidad de que el paciente, al no conocerla, transmita a terceros información que

---

[206] El art. 20.5 del Código Penal establece que no incurrirá en responsabilidad penal: "El que, en estado de necesidad, para evitar un mal propio o ajeno lesione un bien jurídico de otra persona o infrinja un deber siempre que concurran los siguientes requisitos: 1. Que el mal causado no sea mayor que el que se trate de evitar".

[207] Artículo 4.5: *Toda persona tiene derecho a ser informada de sus datos genéticos y otros de carácter personal que se obtengan en el curso de una investigación biomédica, según los términos en que manifestó su voluntad. El mismo derecho se reconoce a la persona que haya aportado, con la finalidad indicada, muestras biológicas, o cuando se hayan obtenido otros materiales biológicos a partir de aquéllos. Se respetará el derecho de la persona a decidir que no se le comuniquen los datos a los que se refiere el apartado anterior, incluidos los descubrimientos inesperados que se pudieran producir. No obstante, cuando esta información, según criterio del médico responsable, sea necesaria para evitar un grave perjuicio para su salud o la de sus familiares biológicos, se informará a un familiar próximo o a un representante, previa consulta del comité asistencial si lo hubiera. En todo caso, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades*.
Artículo 49.2: *Cuando el sujeto fuente haya ejercido el derecho a no ser informado de los resultados de un análisis genético sólo se suministrará la información que sea necesaria para el seguimiento del tratamiento prescrito por el médico y aceptado por el paciente. Cuando esta información sea necesaria para evitar un grave perjuicio para la salud de sus familiares biológicos, se podrá informar a los afectados o a su representante.*

[208] Véase el interesante estudio que hace SANCHEZ CARO, J. sobre la revelación de la información a los parientes consanguíneos en función de la aplicación de los principios de beneficencia, de autonomía, de justicia, y de las virtudes hipocráticas, en SÁNCHEZ-CARO J. y ABELLÁN, F "Información genética y Derecho" en *Medicina Personalizada. Aspectos científicos, bioéticos y jurídicos,* Fundación Salud 2000, 2014, pp. 137-151.

[209] Véase ARCOS VIEIRA, M.ª L., "Consentimiento no informado: reflexiones en torno a la existencia de un "Derecho a no saber" aplicado a la información clínica.", en ARCOS VIEIRA, M.ª L. (directora) *Autonomía del paciente e intereses de terceros: límites,* Thomson-Reuters-ARANZADI, 2016, p. 62.

pueda resultar de interés para ellos. Cierto que este artículo no dispone expresamente nada en cuanto a la eventualidad de que, ante la renuncia a saber, sean informadas las personas vinculadas al paciente por razones familiares o de hecho, y cabría afirmar que esta posibilidad está vetada por el artículo 5.1 LBAP en cuanto sólo permite comunicar a un tercero datos cuando el paciente lo autorice. Sin embargo, no parece que proceda hacer una interpretación literalista de estos artículos. Entendemos que, en cualquier caso, es factible ética y jurídicamente la posibilidad de que el médico comunique los datos a un tercero sin el consentimiento del sujeto cuando concurren razones suficientes (riesgo grave), conozca o no los datos. El procedimiento a seguir sería, en primer lugar, consensuar con el sujeto el momento y forma en el que transmitirá a los familiares consanguíneos la información y, en segundo lugar, ante la negativa a hacerlo, es cuando estará legitimada una actuación de revelación del secreto. Ello por cuanto el derecho a no saber y a que no se comunique a un tercero datos personales no son derechos absolutos y no conlleva de ninguna manera el derecho a que los demás tampoco sepan[210].

Como ha puesto de manifiesto GÓMEZ SÁNCHEZ[211], estos límites al deber de secreto responden a la pretensión de que el reconocimiento de un derecho no lleve, de facto, a una situación de abuso o de uso antisocial del mismo. Resalta que estas medidas tienen como objetivo principal proteger el ejercicio libre de otros derechos o de valores, principios y bienes colectivos igualmente reconocidos por el ordenamiento jurídico. En suma, el derecho a no saber no puede imponerse a derechos fundamentales de un tercero como la vida, la integridad física o la protección de su salud. La protección de estos bienes justifica sobradamente quebrantar el deber de secreto.

X. SECRETO PROFESIONAL DE LOS RESPONSABLES Y ENCARGADOS DE TRATAMIENTO DE DATOS DE SALUD *VS* OBLIGACIÓN DE PERMITIR A LAS AUTORIDADES DE CONTROL EL ACCESO A TODOS LOS DATOS: CONCILIACIÓN.

Propuesta de regulación:

1. El responsable y encargado del tratamiento de datos y quienes intervengan en cualquier fase del tratamiento de los datos, 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.

[210] Véase en este sentido, FEITO GRANDE, L. "Aspectos bioéticos relacionados con la medicina personalizada" en el libro colectivo SÁNCHEZ-CARO J. y ABELLÁN, F., *Medicina personalizada. Aspectos científicos, bioéticos y jurídicos,* Fundación Salud 2000, 2014, pp. 123-124.

[211] GÓMES SÁNCHEZ, Y., voz "Derecho a no saber" en ROMEO CASABONA, C Mª (director) *Enciclopedia de Bioderecho y Bioética,* Tomo I, Comares, S. L., 2011, pp. 597-599.

2. El poder de las autoridades de control estatal y autonómicas para acceder a todos los datos personales en el ejercicio de sus funciones de investigación queda sujeto a las siguientes reglas:

A. Los responsables y encargados del tratamiento de datos personales no estarán obligados a dar a las autoridades de control estatal y autonómicas acceso a los datos de salud, de modo que prevalecerá, al menos inicialmente, el deber de secreto.

B. Los responsable y encargados del tratamiento de datos personales podrán exigir que se precise y se justifique motivadamente qué concretos datos de salud se consideran necesarios por la autoridad de control para el buen fin de la investigación.

C. Cuando los responsables o encargados del tratamiento de datos personales cedan datos de salud, deberán hacerlo con las máximas restricciones posibles y procurando el menor perjuicio para los titulares de los datos, incluso con anonimización cuando de esta forma pueda alcanzarse el fin de la investigación.

D. En todo caso, las autoridades de control estatal y autonómicas no tendrán acceso a los datos de salud en las siguientes áreas: genética, sexualidad y reproducción, enfermedades mentales e infecciosas que puedan perjudicar la vida social o laboral de sus titulares.

3. Las autoridades de control estatal y autonómicas asumen el deber de secreto respecto de los datos a los que accedan y conozcan.

Comentario exegético:

El artículo 4 del RGPD contiene las siguientes definiciones de fichero, responsable y encargado:

> «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
>
> «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento;
>
> «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

El artículo 10 de la LOPD regula de forma individualizada el deber de secreto de quienes tratan datos personales y que acceden lícitamente a los mismos. Con la imposición de este deber de secreto el legislador pretende que los datos personales no puedan conocerse por terceros ajenos al proceso de tratamiento de datos. Este deber de secreto tiene la misma fundamentación jurídica, aunque referido aquí al ámbito estricto

del tratamiento de los datos personales, de manera que el responsable del fichero y, cualquier persona que intervenga en el tratamiento, está obligado al mantener el deber de secreto respecto de los datos que trata. En suma, en el ámbito informático también se genera un deber de confidencialidad similar al de las profesiones u oficios sanitarios en el ámbito asistencial y de salud pública, pero que recae sobre las entidades responsables de los ficheros de datos y sobre los encargados de su tratamiento.

Este deber de secreto, no obstante, cede ante procesos de investigación de la autoridad de control creada por el RGPD. El artículo 4 del RGPD define la «autoridad de control» como la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51, el cual dispone que

> Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

A su vez, el artículo 58. 1. e) del RGPD establece que

> la autoridad de control, como poder de investigación, podrá obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones.

No obstante, el artículo 90 del RGPD dispone que

> "Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e)[212] y f)[213], en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto."

El considerando 164 del RGPD indica que "Por lo que respecta a los poderes de las autoridades de control para obtener del responsable o del encargado del tratamiento acceso a los datos personales y a sus locales, los Estados miembros pueden adoptar por ley, dentro de los límites fijados por el presente Reglamento, normas específicas con vistas a salvaguardar el deber de secreto profesional u obligaciones equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con el deber de secreto profesional. Lo anterior se entiende sin perjuicio de las obligaciones existentes para los Estados miembros de adoptar normas sobre el secreto profesional cuando así lo exija el Derecho de la Unión."

[212] Acceso a todos los datos personales.
[213] Acceso a locales e instalaciones.

El artículo 45 del anteproyecto de nueva LGPD establece como autoridad de control estatal a la AEPD y en el artículo 58 prevé la creación de autoridades de control autonómicas que ejercerán en el ámbito de la Comunidad Autónoma las funciones que establecen los artículos 57 y 58 del RGPD. Parece más adecuado a nivel autonómico crear autoridades de control independientes por sectores específicos (asistencial, investigador, etc.).

XI. COMUNICACIÓN DE DATOS AL MINISTERIO FISCAL Y A LOS DEFENSORES DEL PUEBLO Y SECRETO PROFESIONAL

Propuesta de regulación:

Los fiscales y los defensores del pueblo a quienes se comunique datos de salud en el ejercicio de las funciones que tienen atribuidas, así como el personal de estos órganos que accedan a dichos datos en el ejercicio de su función, se obligan, por el solo hecho de la comunicación, a observar el deber de secreto profesional.

Comentario exegético:

El artículo 11.2 de la todavía vigente LOPD enumera una serie de supuestos en los que es legítimo comunicar datos a un tercero sin consentimiento previo del interesado. Así, en lo que aquí interesa, como destinatarios de los datos cita al ministerio fiscal y a los Defensores del Pueblo estatal y autonómicos. La cesión o comunicación de datos de salud a estos órganos también tiene amparo en el artículo 9. 2.f) del RGPD en cuanto permite el tratamiento de datos sin el consentimiento del interesado cuando "*El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.*" En la redacción de la versión del RGPD de junio de 2015 figuraba "el ejercicio o defensa de un derecho en un procedimiento judicial". Es decir, quedaba la excepción limitada estrictamente al ámbito judicial. Empero, en la redacción definitiva finalmente se ha sustituido "*la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial*", y reclamaciones pueden formularse en vía administrativa o ante órganos no jurisdiccionales, así pues, fuera del ámbito judicial. En efecto, advierte el considerando 52 RGPD que "*debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.*" Las quejas interpuestas ante los defensores del pueblo son técnicamente reclamaciones extrajudiciales.

Pues bien, el citado artículo 11 de la LOPD establece en su apartado 5 que "*aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.*" y ya conocemos que el artículo 10 impone al responsable del fichero y quienes intervengan

en cualquier fase del tratamiento de los datos de carácter personal al deber de secreto profesional respecto de los mismos y al deber de guardarlos.

Afirma la STS de 7 de noviembre de 2009 -RJ/2009/8046- que esta "excepción sólo se predica de comunicaciones de datos con los concretos destinatarios que se indican (Ministerio fiscal, Jueces y Defensor del Pueblo) y en el ejercicio de sus funciones, lo que necesariamente implica una comunicación directa y que la misma se produzca a requerimiento del destinatario en el ejercicio de sus funciones, circunstancias que ha de valorar el responsable del fichero para emitir la correspondiente comunicación de datos al amparo de dicha excepción, que, además y por su propia naturaleza, ha de interpretarse en sentido estricto".

Disponen sistemáticamente las leyes reguladoras de los Defensores del Pueblo que las investigaciones que realice el Defensor del Pueblo o el personal dependiente del mismo se producirán dentro de la más estricta reserva. De este mandato puede inferirse que tanto el Defensor del Pueblo como el personal de su oficina quedan obligados al secreto respecto de todos los datos que lleguen a conocer en el curso de las investigaciones que practiquen. No obstante, no existe en dichas leyes una declaración expresa sujetando a estas personas al deber de secreto respecto de los datos personales que se comuniquen para la realización de las investigaciones. Por ello, no nos parece reiterativa una norma como la que proponemos que expresamente establezca el deber de secreto.

El artículo 50 de la Ley 50/1981, 30 diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal, establece que "Los miembros del Ministerio Fiscal guardarán el debido secreto de los asuntos reservados de que conozcan por razón de su cargo." En la expresión "asuntos reservados" entiendo que deben comprenderse los datos de salud que pueda conocer en el ejercicio de las funciones que tiene atribuidas. Empero, en los dos artículos (70 y 71) dedicados al personal que sirve a la institución nada se dice respecto del deber de secreto. Por ello, parece oportuno extender el deber de secreto a este personal.

XII. FORMACIÓN CONTINUADA Y PUBLICIDAD DE LAS TRANSFERENCIAS DE VALOR DE LA INDUSTRIA BIO-FARMACÉUTICA A PROFESIONALES SANITARIOS *VS* INTIMIDAD.

Propuesta de regulación:

Sin necesidad de recabar previamente el consentimiento de los interesados, serán de declaración pública e individualizada las transferencias de valor (colaboración económica para reuniones científicas y profesionales; prestación de servicios) realizadas a profesionales sanitarios para actividades de formación continuada, incluidas las desarrolladas por las sociedades científicas, aunque no hayan sido percibidas directamente por el profesional sanitario.

Comentario exegético:

La formación continuada de los profesionales sanitarios es una tarea ineludible al objeto de proporcionar la mejor atención sanitaria y de salud pública a la población. Los gastos inherentes a las actividades de formación continuada (cuotas de inscripción, desplazamientos, alojamientos, etc.) vienen siendo financiadas en su gran mayoría por las sociedades científicas a través de sus propios fondos y principalmente por aportaciones de la industria bio-farmacéutica. La transparencia y publicidad que el artículo 11 de la LGSP exige a las organizaciones científicas y profesionales se ha de traducir en que sean públicas las colaboraciones económicas entre sociedades, profesionales y empresas y laboratorios farmacéuticos en el campo de la formación continuada. Concretamente, el artículo 78.4 del Real Decreto Legislativo 1/2015, de 24 de julio, que aprueba el Texto Refundido de la Ley del Medicamento establece que:

> las ofertas de premios, becas, contribuciones y subvenciones a reuniones, congresos, viajes de estudio y actos similares por cualquier persona, física o jurídica, relacionada con la fabricación, elaboración, distribución, prescripción y dispensación de medicamentos y productos sanitarios, se harán públicas en la forma que se determine reglamentariamente y se aplicarán exclusivamente a actividades de índole científica cuando sus destinatarios sean profesionales sanitarios o las entidades en que se asocian. En los programas, publicaciones de trabajos y ponencias de reuniones, congresos y actos similares se harán constar la fuente de financiación de los mismos y los fondos obtenidos de cada fuente. La misma obligación alcanzará al medio de comunicación por cuya vía se hagan públicos y que obtenga fondos por o para su publicación.

Farmaindustria aprobó en el año 2016 un Código de Buenas Prácticas, con el carácter de norma autorregulatoria, por el que, sin recabar previamente el consentimiento de los interesados, se obliga a hacer públicas de forma individualizada las transferencias de valor (donaciones, cuotas de inscripción, desplazamientos, alojamientos, etc, en reuniones científicas y profesionales; prestación de servicios) que la industria bio-farmacéutica realice a los profesionales sanitarios para financiar actividades formativas, incluidas las desarrolladas por las sociedades científicas, aunque no hayan sido percibidas directamente por el profesional.

Los datos económicos y la identificación del profesional que recibe las aportaciones económicas para su formación continuada no son datos de salud conforme a la descripción que de estos hace el considerando 35 del RGPD y a la definición contenida en el artículo 4.15. No encajan, por tanto, en el régimen de protección establecido en el artículo 9 para datos sensibles, como los de salud. Pero sí encajan en la definición de "datos personales" que hace el citado artículo 4 en su apartado 1 y, por ende, en el régimen de protección que con carácter general establece el RGPD para todo tipo de datos personales. Pues bien, aunque se salga estrictamente del tema que nos ocupa, ello me impulsa a incorporar este último apartado a este estudio con el ánimo de favorecer la necesaria transparencia en las relaciones de la industria farmacéutica con los profesionales sanitarios.

El Informe del Gabinete Jurídico, núm. 2016-0172 (REF 143318/2016), de 22 de abril de 2016, de la Agencia Española de Protección de Datos, al analizar las obligaciones que se crea Farmaindustria con el Código de Buenas Prácticas, concluye que, de conformidad con el artículo 7 f) de la Directiva 95/46 (actualmente, artículo 6. f) del RGPD), existe un interés legítimo[214] de las empresas sujetas al Código, de forma que no es necesario el consentimiento para la publicación de forma individual de las transferencias de valor a los profesionales sanitarios. Tras esta afirmación, añade que *"Si bien estas circunstancias permitirían considerar que la ponderación exigida por el artículo 7 f) de la Directiva 95/46/CE puede realizarse en favor de la publicación, sería conveniente que a las mismas se añadiesen medidas que impidan un tratamiento posterior de los datos que pueda alejarse dela finalidad perseguida, dado que el acceso a la información permitiría a quienes la conocieran llevar a cabo tratamientos adicionales basados no tanto en la finalidad de transparencia en relación con las transferencias de valor sino en la elaboración de perfiles de los profesionales que reciben tales transferencias. A tal efecto, sería conveniente que se aplicaran al sitio web en que se lleve a cabo la publicación protocolos que eviten su indexación a través de motores de búsqueda. Del mismo modo, sería relevante en aras a garantizar la proporcionalidad de la medida que en el propio sitio web se indicase claramente que la finalidad de la publicación es la indicada en la consulta y que de la misma no se deriva una habilitación general para que quienes accedan al sitio web puedan llevar a cabo un tratamiento adicional de los datos de los profesionales, tales como su cruce con las informaciones publicadas en los sitios web de otros asociados."*

No obstante, en nuestra opinión, una información pública en Internet que no se pueda indizar en los motores de búsqueda es una información inexistente. La condición de que la página web no sea indizable no casa bien con la publicidad que se busca de las transferencias de valor de la industria bio-farmacéutica a profesionales sanitarios. Sin embargo, es cierto que los profesionales sanitarios señalados en esa publicidad deberían estar protegidos de posibles usos abusivos de esa información en su contra, quizá mediante la localización de esa publicidad durante periodos limitados de tiempo.

[214] En cuanto a la delimitación del interés legítimo invocado por la consultante, se indica en el escrito remitido a la Agencia que "la publicación individualizada de las transferencias de valor persigue, disminuir el riesgo de percepción sobre la influencia que pueda haber recibido el profesional sanitario, promueve una cultura de integridad en las transacciones con los profesionales sanitarios y la confianza del público y los pacientes en la integridad e independencia del profesional sanitario, algo esencial para generar confianza en dichas relaciones y para su buen funcionamiento". Igualmente se indica que con ello se persigue "asegurar que los laboratorios farmacéuticos cumplan con los estrictos límites que establece tanto la legislación (nacional como comunitaria) y el propio Sistema de Autorregulación en materia de promoción de medicamentos", evitando "que las interacciones de la industria farmacéutica con los profesionales sanitarios puedan constituir una infracción de la Directiva 2001/83/ CE, por la que se establece un Código comunitario para medicamentos de uso humano y Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el Texto Refundido de la Ley de Garantías y uso racional de los medicamentos y productos sanitarios".