

LA PROTECCIÓN DE LOS DATOS SANITARIOS EN EUROPA Y LA COMISIÓN DE DELITOS CONTRA LA INTIMIDAD EN EL ÁMBITO CLÍNICO

Silvia Mendoza Calderón

Profesora Titular acreditada de Derecho penal

Contratada Doctora en la Universidad Pablo de Olavide de Sevilla.

SUMARIO: I. INTRODUCCIÓN. II. CONCEPTO DE DATOS SANITARIOS EN EUROPA Y PRINCIPIOS QUE CONFORMAN SU TRATAMIENTO. 2.1 La relevancia de los datos sanitarios en la normativa europea. 2.2 Principios reguladores en materia de protección de datos sanitarios. III. ALGUNAS CONSIDERACIONES SOBRE LA REPERCUSIÓN PENAL DE LA FILTRACIÓN DE DATOS SANITARIOS: COMISIÓN DE DELITOS CONTRA LA INTIMIDAD. 3.1 El delito de utilización de datos personales sin estar autorizado (art. 197.2 CP). 3.2 El delito de revelación de secreto profesional (art. 199 CP). IV. CONCLUSIONES. V. BIBLIOGRAFÍA.

RESUMEN

El presente trabajo analiza el alcance de la protección de los datos sanitarios en el entorno de la Unión Europea, así como la trascendencia de la filtración y utilización ilegal de dichos datos, cuando ésta tenga tal relevancia que pueda llegar a constituir delitos contra la intimidad de las personas.

Asimismo, se prestará especial atención al secreto profesional médico, así como se examinarán cuestiones relativas al tratamiento del error del sanitario en este ámbito.

PALABRAS CLAVE

Datos sanitarios, Unión Europea, delitos contra la intimidad.

ABSTRACT

This paper studies the scope of health data's protection in the European Union, as well as the importance of the disclosure and illegal use of such data, when it has such relevance that it may constitute privacy offences.

Also, particular attention will be paid to medical professional secrecy, as well as consideration of issues relating to the handling of medical errors in this area.

KEYWORDS

Health data, European Union, privacy offences.

I. INTRODUCCIÓN

Los datos sanitarios siempre han sido considerados como datos personales muy sensibles y dotados de una especial protección. En el año 2015, la prensa británica informaba que a través de Internet, empresas como “Google” tendrían acceso a un millón y medio de historias clínicas, ya que el servicio sanitario de Gran Bretaña (*National Health Service*) las habría cedido encriptadas para desarrollar una app y detectar enfermedades hepáticas, pudiendo consultarse historiales clínicos en los que figurarían abortos, sobredosis, adicciones, trasplantes o incluso el sida, con el objetivo de controlar sus analíticas para evitar muertes por fallos del riñón (15.000 defunciones al año que se podrían evitar)¹.

Asimismo, en España, en 2014, se habría investigado por parte de la Consejería de Sanidad de Madrid la cesión de datos de pacientes por un hospital público a una clínica privada, para que ésta se pusiera en contacto con aquellos pacientes que estaban en listas de espera, para citarles, cuando era el propio hospital quien debía hacerlo², siendo denunciado este hecho asimismo a la Agencia Española de Protección de Datos, por organizaciones como FACUA.

Hay que partir en esta cuestión, que una asistencia sanitaria adecuada requiere en primer lugar, de una información correcta sobre aspectos de la vida y la salud del paciente y una conservación perfecta de los mismos. Junto al **interés particular** de cada uno en su propia salud, ésta constituye un **bien social** que el Estado ha de promover y preservar mediante las campañas de prevención y vacunación mediante la investigación. Por otra parte, hay que recalcar que normalmente es preciso revelar al profesional médico **datos extremadamente confidenciales**, aspectos de nuestra vida que en condiciones normales no revelaríamos a nadie³.

1 Cfr. <http://www.redaccionmedica.com/secciones/sanidad-hoy/el-doctor-google-tiene-acceso-a-1-5-millones-de-historias-clinicas-3036>, consultada en mayo 2016.

2 <http://www.rtve.es/noticias/20140813/consejeria-sanidad-madrid-investiga-cesion-datos-pacientes-clinica-privada/992186.shtml>, consultada en mayo 2016.

3 SERRANO PÉREZ, “La protección de los datos sanitarios en Europa. La historia clínica”, en https://www.uclm.es/actividades0506/seminarios/proteccion_datos/pdf/datos_sanitarios.pdf, consultada en junio 2016, afirmando que estarían implicados el derecho a la salud del art. 43 CE, derecho a la intimidad personal y familiar del art. 18.1 CE, el derecho a la vida del art. 15 CE y la protección de datos de carácter personal del art. 18.4 CE.

Conforme a la *Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre*, el derecho a la protección de datos de carácter personal del art. 18.4 CE, de acuerdo con los textos internacionales, consistiría en **un poder de disposición y de control sobre los datos personales que faculta para decidir sobre ellos**⁴, articulándose a través de un contenido esencial **que incluiría el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos, y el derecho a acceder, rectificar y cancelar dichos datos**.

En lo que respecta a esta serie de normativa internacional que regularía este derecho, se encontraría el *Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* (ratificado por España el 27 de enero de 1984), la *Carta Europea de Derechos Fundamentales*, de 7 de diciembre de 2006, que eleva a la **categoría de derecho fundamental el derecho a la protección de datos personales**, el *Convenio sobre Derechos Humanos y Biomedicina (Convenio de Oviedo) de 1997, relativo a los derechos humanos y a la biomedicina*⁵.

En el entorno europeo, tendrían notable relevancia el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* y por el que se deroga la Directiva 95/46/CE⁶; la *Directiva (UE) 2016/680 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos* (y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo) y la *Directiva 2011/24/*

4 SERRANO PÉREZ, “La protección de los datos sanitarios en Europa. La historia clínica”, en https://www.uclm.es/actividades0506/seminarios/proteccion_datos/pdf/datos_sanitarios.pdf, consultada en junio 2016.

5 Cfr. ROMEO CASABONA, (Coordinación), *El Convenio de Derechos Humanos y Biomedicina. Su entrada en vigor en el ordenamiento jurídico español*, Bilbao-Granada 2002, pp. 174 s.

6 Directiva 95/46, de 24 de octubre relativa a la protección de las personas físicas y en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (derogada).

UE, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.

En lo relativo al marco normativo nacional, hay que referirse a lo dispuesto por la *Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*⁷; la *Ley 41/2002, de 14 de noviembre, básica reguladora de los derechos del paciente*; la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* y la *Ley 14/86, de 25 de abril, Ley General de Sanidad*.

En el presente estudio se analizará el alcance de la protección de los datos sanitarios en el entorno de la Unión Europea, así como la trascendencia de la filtración y utilización ilegal de dichos datos, cuando ésta tenga tal relevancia que pueda llegar a constituir delitos contra la intimidad de las personas.

Asimismo, se prestará especial atención al secreto profesional médico, así como se examinarán cuestiones relativas al tratamiento del error del sanitario en este ámbito.

II. CONCEPTO DE DATOS SANITARIOS EN EUROPA Y PRINCIPIOS QUE CONFORMAN SU TRATAMIENTO

2.1 La relevancia de los datos sanitarios en la normativa europea

El Considerando 45 del *Convenio 108 del Consejo de Europa, de 28 de enero de 1981*, estimaba datos sanitarios a aquellas **informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo. Igualmente se incluía en estos datos las informaciones relativas al abuso de alcohol o al consumo de drogas**⁸.

La *Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016*, establece que entre **los datos personales relacionados con la**

salud se deberían incluir todos los datos relativos al estado de salud del interesado (estado de la salud física o mental pasado, presente o futuro, incluidos los datos personales recopilados durante la inscripción de una persona física a efectos de la prestación de servicios de asistencia sanitaria)⁹.

Asimismo, tendrían esta consideración **todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluidos los datos genéticos y las muestras biológicas, y cualquier información relativa a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, ya sea un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro**.

Se estimarían como **datos genéticos** todos los datos personales relacionados con las características genéticas de una persona física que se hayan heredado o adquirido y que aporten información única sobre la fisiología o la salud de esa persona física, y que resultan de análisis de una muestra biológica de la persona física de que se trate, en particular cromosómicos, del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o de análisis de cualquier otro elemento que permita obtener información equivalente¹⁰.

⁹ Cfr. SERRANO PEREZ, *ul.op.cit.*, pp. 386 ss, indica que en relación a los datos sanitarios regiría el principio de limitación personal en cuanto a la necesidad de tratar esas categorías de datos, cuando ello sea preciso en orden a las prevención y prestación de asistencia sanitaria o gestión de servicios de la misma índole. Para este supuesto, tales tratamientos solamente podrán ser efectuados por un facultativo sanitario sometido a secreto profesional o bien por otra persona sujeta igualmente a la misma obligación, siguiendo el criterio mantenido por las recomendaciones en materia de Salud del Consejo de Europa. Se recoge que en la normativa europea se maneja un concepto amplio de dato sanitario puesto que sensibiliza tanto los datos relativos a cuestiones sanitarias en sentido estricto como los relativos a la administración sanitaria.

¹⁰ Cfr. Sobre este concepto, SÁNCHEZ CARO, ABEILLÁN, *Datos de salud y datos genéticos. Su protección en la Unión Europea y en España*, Granada, 2004, pp. 135 s. Cfr. Igualmente, ROMEO CASABONA, "El tratamiento y la protección de los datos genéticos", *Gen-Ética*, Barcelona 2003, pág. 244, señalando que los datos genéticos deben ser protegidos frente a terceras personas, incluso en el caso de familiares, aunque esos terceros tengan un interés objetivo en conocer esa información. No obstante, una vez asentada la relevancia del derecho de la persona sobre su propia información genética, sería posible encontrar restricciones a este derecho en determinadas circunstancias en las que exista una adecuada justificación.

⁷ Cfr. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

⁸ Cfr en relación a la trascendencia de los datos sanitarios, ROMEO CASABONA, "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, julio-diciembre, 1993, p. 5.

Por otra parte, tendrán el carácter de datos **biométricos**, aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

En relación al tratamiento de estos datos sanitarios, la *Directiva 2016/680, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales*, dispone en su artículo 10 que el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento **de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales** de una persona física **solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado** y únicamente cuando: lo autorice el Derecho de la Unión o del Estado miembro; **sea necesario para proteger los intereses vitales del interesado o de otra persona física**, o dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

2.2 Principios reguladores en materia de protección de datos sanitarios

En materia de protección de datos personales y su tratamiento, en lo que respecta a los principios recogidos en la normativa nacional de protección de datos y su aplicación en el campo sanitario, cobran notable importancia **el principio de confidencialidad, el principio de adecuación y pertinencia, el principio de exactitud, el principio de cancelación, el principio de lealtad y el principio de seguridad**¹¹.

El principio de confidencialidad implica la existencia de consentimiento informado del interesado para el tratamiento de los datos sobre la salud,

estableciendo la confidencialidad como el elemento esencial que le convence para la entrega de datos tan sensibles como los datos sobre la salud¹².

El principio de adecuación y pertinencia conlleva que los datos sean **adecuados, pertinentes y no excesivos** en relación con las finalidades para las que se hayan recabado para garantizar una asistencia adecuada al paciente¹³.

El principio de exactitud significa el sostenimiento de datos exactos y **puestos al día** para que respondan con veracidad a la situación real del interesado, dado el interés vital que tiene el interesado en adecuar las informaciones incluidas en su historia clínica con su realidad¹⁴.

El principio de cancelación significa que debe producirse la cancelación de los datos cuando hayan dejado de ser necesarios o pertinentes en relación con la finalidad para la que se recogieron. Puede que sea preciso mantener los datos sanitarios en caso de tratamientos médicos prolongados o enfermedades crónicas en las que nunca llega a romperse la conexión entre la finalidad y el mantenimiento del dato¹⁵.

El principio de lealtad exige que la información sanitaria, no puede recogerse **de forma desleal, fraudulenta o ilícita**, y el principio de seguridad sería una garantía **de la integridad de la información, de la disponibilidad de la misma y de su confidencialidad**¹⁶.

12 SERRANO PÉREZ, *ul.op.cit.*

13 SERRANO PÉREZ, *ul.op.cit.* Cfr. Igualmente, ANDREU MARTÍNEZ, ALARCÓN SEVILLA, SALCEDO HERNÁNDEZ, SORO MATEO, “Sanidad electrónica e intercambio de información sanitaria en Europa a la luz de la nueva regulación sobre protección de datos personales”, en *Derecho y Salud*, Vol. 24 Extraordinario XXIII Congreso 2014, pp. 265 ss, señalan que si bien puede acudir al consentimiento explicito o realizar un tratamiento de datos de salud sin dicho consentimiento cuando esté en juego un interés vital del sujeto, el supuesto en el que de forma ordinaria debería basarse el tratamiento de datos de salud en el marco de la prestación de asistencia sanitaria es siguiendo una serie de requisitos para que pueda servir de fundamento al tratamiento: que éste sea *necesario* para conseguir la *finalidad* establecida en el precepto, a saber, la prevención, el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico, o la gestión de los servicios sanitarios; y que, además, se realice por un *profesional sanitario* sujeto al *secreto profesional* (u otra persona sujeta a secreto médico profesional u otro equivalente).

14 SERRANO PÉREZ, *ul.op.cit.*

15 SERRANO PÉREZ, *ul.op.cit.*

16 SERRANO PÉREZ, *ul.op.cit.* Cfr. Igualmente, ANDREU MARTÍNEZ, ALARCÓN SEVILLA, SALCEDO HERNÁNDEZ, SORO MATEO, “Sanidad electrónica e intercambio de información sanitaria en Europa a la luz de la nueva regu-

11 SERRANO PÉREZ, “La protección de los datos sanitarios en Europa. La historia clínica”, en https://www.uclm.es/actividades0506/seminarios/proteccion_datos/pdf/datos_sanitarios.pdf, consultada en junio 2016.

De esta forma, se concibe a los **datos de salud** como todos *aquellos datos de carácter personal que indiquen la situación de salud o enfermedad de un individuo*, es decir, los relativos a la salud o los que contengan conexión con fines relacionados con la salud (física o mental), aunque sean tratados en ámbitos no estrictamente sanitarios (seguros, investigación...), siendo indiferente que el dato médico obre en el expediente del paciente o en la historia clínica, porque aunque en ésta haya aportaciones intelectuales del médico, en la misma se incluyen también datos que afectarían a la intimidad del paciente¹⁷.

Por otra parte, se define a la **historia clínica** como el soporte, informatizado o no, que contiene la información clínica del sujeto, constituyendo los datos relativos a la salud que forman parte de la historia clínica parte de un fichero informático o manual estructurado que va a estar conformado por el conjunto de historias clínicas de cada centro asistencial. Así, la *Ley 41/2002, de 14 de noviembre, básica reguladora de los derechos del paciente*, recoge la creación y la existencia de la historia clínica como un derecho del paciente y como un deber por parte del centro o institución sanitaria (artículos 15 y 14.2)¹⁸.

lación sobre protección de datos personales”, en *Derecho y Salud*, Vol. 24 Extraordinario XXIII Congreso 2014, pp. 265 ss, indican en torno a la continuidad de la asistencia sanitaria transfronteriza, que los datos que deben incluirse en un historial clínico para ser compartidos por los profesionales sanitarios, hay que partir como se ha señalado repetidamente de los principios de calidad y proporcionalidad. Los datos de salud que se recaben han de ser adecuados, pertinentes y limitados al número necesario en relación con la finalidad para la que se tratan. Una de las cuestiones en las que incide especialmente la nueva regulación en materia de protección de datos es precisamente la minimización en el tratamiento, de ahí que el mencionado precepto precise que los datos sólo se tratarán cuando los fines no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales.

17 GARCÍA SANZ, “El secreto profesional en el ámbito sanitario”, en *ANALES DE LA FACULTAD DE DERECHO*, 22; diciembre 2005, pp. 187-211.

18 Cfr. GARRIGA DOMINGUEZ (Dirección), “Historia clínica y protección de datos personales: recomendaciones y propuestas en torno al uso de la información”, *Informe elaborado en el marco del laboratorio de la sociedad de la información y derechos humanos dentro del programa “el tiempo de los derechos”, consolidar-ingenio 2010, por el Grupo de investigación HI13 de la Universidad de Vigo, noviembre 2010*, pp. 4 ss. GONZÁLEZ GARCÍA, “El derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos”, *Derecho y salud*, vol.24, 2014 pp.27 ss, indica que la historia clínica es un instrumento que sirve para almacenar y organizar toda la información del paciente relativa a los procesos asistenciales, en ella queda incluida la identificación de los profesionales que le serán los que estén legitimados para acceder a ella, obligando a los centros a establecer mecanismos de seguridad que garanticen la intimidad del paciente. Además es una herramienta básica para la investigación biomédica, la educación de estudiantes y la formación médica continua.

Respecto al acceso a la historia clínica, **éste** se permite a los profesionales asistenciales que realizan el diagnóstico o el tratamiento del paciente, teniendo la obligación de cumplimentar la historia clínica, fechando y firmando la información incorporada, identificándose a la persona que lo realiza. También pueden acceder a las misma, el personal de administración y gestión, siempre en relación a los datos conectados con sus propias funciones. La historia clínica también puede tener otros usos (judiciales, epidemiológicos, de salud pública, de investigación o de docencia), con la obligación de disociar los datos de identificación personal, de los clínico-asistenciales, de manera que quede garantizado el anonimato, salvo que el paciente otorgue su consentimiento para no disociarlo. Otro colectivo sanitario, al que se permitiría el acceso a las historias clínicas, serían aquellos que ejercen funciones de inspección, evaluación, acreditación y planificación, pero limitado al cumplimiento de sus funciones de comprobación¹⁹.

Asimismo, se habría destacado que los **datos genéticos** deben ser considerados como datos “sensibles” o “supersensibles”, al ser incluso más vulnerables que el resto de datos de salud, ya que a partir de ciertas muestras orgánicas sometidas a determinados análisis genéticos puede obtenerse información que podría convertir al ser humano en “ciudadano transparente” o de “cristal” y su revelación supondría una lesión a la intimidad. Se alude a un “derecho a la intimidad genética” incluyendo también un derecho a “no saber”²⁰.

III. ALGUNAS CONSIDERACIONES SOBRE LA REPERCUSIÓN PENAL DE LA FILTRACIÓN DE DATOS SANITARIOS: COMISIÓN DE DELITOS CONTRA LA INTIMIDAD

Como ha indicado la doctrina, el incumplimiento de deberes por parte del personal sanitario puede

19 GONZÁLEZ GARCÍA, *ul.op.cit*, pp.27 ss. Cfr. igualmente sobre la historia clínica electrónica en la Ley de Autonomía del Paciente, GÓMEZ ÁLVAREZ, “La transmisión de datos médicos en la cooperación judicial penal y policial en el seno de la Unión Europea: en particular, la transmisión de la historia clínica”, en COLOMER HERNÁNDEZ (Director), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Cizur Menor, 2015, pp. 566 ss.

20 GARCÍA SANZ, “El secreto profesional en el ámbito sanitario”, en *ANALES DE LA FACULTAD DE DERECHO*, 22; diciembre 2005, pp. 187-211. ROMEO CASABONA, C., *El tratamiento y la protección de los datos genéticos*, en *Genética*, Ariel, Barcelona, 2003, pág. 240.

llegar a constituir infracciones de carácter penal, siendo una de las formas más graves la vulneración del secreto médico profesional o de la obligación de preservar y custodiar la confidencialidad e intimidad del paciente²¹.

Se habría destacado que a efectos de la protección penal, aparecería un concepto específico de “profesional” en este ámbito, siendo un elemento esencial “el deber de sigilo” respecto a la intimidad del sujeto pasivo que debe tener el profesional a partir de dos notas esenciales como serían por una parte, el carácter necesario de la prestación de servicios (condición del profesional como confidente necesario) y por otra, la reglamentación jurídica de dicha profesión donde se regularía el deber de sigilo de forma preceptiva (código ético o normas deontológicas)²².

GARCÍA SANZ habría afirmado que el deber de secreto profesional en el ámbito sanitario encontraría también su fundamento en normas ético-corporativas, si bien sería preciso deslindar el plano deontológico y jurídico, ya que aunque los profesionales deben adecuar su actuación profesional al Código Deontológico, las pretensiones que frente a ellos se ejerciten por vía judicial, deberán basarse normalmente en la vulneración de una ley²³.

En este sentido, se recoge que una de las primeras cuestiones a analizar es que se utilizan en este campo en forma indistinta términos como los de privacidad, confidencialidad, protección de datos que, aunque tendrían conexión con la intimidad, no serían absolutamente coincidentes²⁴. Siguiendo a ROMEO CASABONA, la intimidad²⁵ vendría constituida por “aquellas manifestaciones de la personalidad individual (o familiar) cuyo conocimiento o desarrollo quedan reservados a su titular o sobre las que ejerce alguna forma de control cuando se ven implicados

terceros”, mientras que la privacidad²⁶ sería el “el derecho de los individuo, grupos o instituciones a determinar por ellos mismos, cuándo, cómo y cuánta información acerca de sí es comunicada a otros.

Se considera en este sentido que la intimidad quedaría reducida al “núcleo duro” de la personalidad, esa zona íntima que queda reservada a una persona o a un círculo restringido de personas (datos de salud, sexuales, raciales...), mientras que en la privacidad se incluirían datos no tan sensibles pero de un ámbito de vida particular²⁷.

GARCÍA SANZ indica asimismo que la *confidencialidad*, cabría concebirla como una “actitud que se le pide al sujeto conocedor del dato o hecho de la intimidad o privacidad de la persona” y supondría “la obligación del profesional de mantener en secreto cualquier información proporcionada por el paciente, no pudiendo revelársela a un tercero sin su permiso específico”. La confidencialidad sería un concepto próximo a la intimidad, de manera que cuanto más íntimo sea el dato, sería preciso un mayor grado de confidencialidad²⁸.

Del mismo modo, también habría que diferenciar la intimidad del *derecho a la protección de datos de carácter personal*, englobando un “derecho fundamental a la protección de datos”, denominado “libertad informática” diferenciado del derecho a la intimidad²⁹.

26 GARCÍA SANZ, *ul.op.cit.*, pp. 187-211., citando a LÓPEZ DÍAZ, E., *El derecho al honor y el derecho a la intimidad. Jurisprudencia y doctrina*, Dykinson, Madrid, 1996, pág. 205

27 GARCÍA SANZ, *ul.op.cit.*, pp. 187-211.

28 GARCÍA SANZ, *ul.op.cit.*, pp. 187-211.

29 GARCÍA SANZ, *ul.op.cit.*, pp. 187-211. Cfr. MATA Y MARTÍN, “La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías”, *Revista penal*, num. 18, 2006, pp. 219 ss. Que indica tres grandes ámbitos a través de los cuales se dispensa protección a este bien jurídico (citando a ROMEO, *Comentarios al Código penal, Parte Especial II*. DÍEZ RIPOLLES/ROMEO CASABONA (coordinadores), Valencia, 2004, págs. 692 y ss.. En primer término estaría la intimidad como reducto de la personalidad en la vida privada, tutela de ciertos ámbitos en los que el interesado puede manifestar su oposición frente a injerencias no deseadas, como ámbito tradicional de la intimidad. En segundo lugar se encuentra la intimidad en su manifestación de confidencialidad compartía, tratándose de sectores en los que intervienen terceros pero a los cuales se les obliga a guardar reserva. Finalmente estaría la intimidad en relación con el procesamiento y comunicación de datos a través de las modernas tecnologías de la información y de la comunicación. Este último caso se refiere a la tutela de las informaciones de carácter reservado que han sido almacenadas o procesadas en un fichero o archivo, es la tutela penal de datos.

21 Cfr. FERNÁNDEZ PANTOJA, “El delito de revelación de secretos en el ámbito sanitario”, en <http://libros-revistas-dercho.vlex.es/vid/oacute-secretos-mbito-sanitario-219796997>, pp. 287-321, consultada en diciembre 2016.

22 Cfr. FERNÁNDEZ PANTOJA, *ul.op.cit.*, pp. 287-321, consultada en diciembre 2016.

23 GARCÍA SANZ, “El secreto profesional en el ámbito sanitario”, en ANALES DE LA FACULTAD DE DERECHO, 22; diciembre 2005, pp. 187-211.

24 GARCÍA SANZ, *ul.op.cit.*, pp. 187-211.

25 GARCÍA SANZ, “El secreto profesional en el ámbito sanitario”, en ANALES DE LA FACULTAD DE DERECHO, 22; diciembre 2005, pp. 187-211., citando a ROMEO CASABONA, C., *El tratamiento y la protección de los datos genéticos*, en Gen-Ética, Ariel, Barcelona, 2003, pág. 240.

Desde este punto de vista, el derecho a la protección de datos personales sería independiente y autónomo respecto al derecho a la intimidad y abarcaría una mayor amplitud de situaciones, pues protegería datos personales sean íntimos o no, bastando que sean datos que identifiquen o permitan la identificación de una persona. Por otra parte, el concepto de *secreto profesional*, implicaría un derecho de autodeterminación del paciente y su derecho fundamental a la intimidad, entendiendo al secreto médico como “*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*”³⁰.

De esta forma, MUÑOZ CONDE habría incidido en que el derecho a la intimidad tendría también un sentido positivo, en el sentido de que se trataría no solo de proteger lo secreto, sino de proteger el derecho al control de aquellos que afectando a la privacidad, puedan ser o no conocidos por otras personas, pero sobre los que en cualquier caso el sujeto tiene derecho a decidir la forma en la que esos datos pueden ser revelados y hasta qué punto³¹.

3.1 El delito de utilización de datos personales sin estar autorizado (art. 197.2 CP)

En el artículo 197 del Código penal, tras la reforma efectuada por la *Ley orgánica 1/2015, de 30 de marzo*, se dispone que el que, **para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación**, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Las mismas penas se impondrán al que **sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen**

30 GARCÍA SANZ, “El secreto profesional en el ámbito sanitario”, en ANALES DE LA FACULTAD DE DERECHO, 22; diciembre 2005, pp. 187-211.

31 MUÑOZ CONDE, “Falsedad documental y secreto profesional en el ámbito sanitario”, en *Derecho y Salud*, Vol. 4, num. 2, Julio-Diciembre, 1996, pp. 147 ss.

registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a **quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero, aplicándose la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas**³².

Por otra parte, estos hechos serán castigados con una pena de prisión de tres a cinco años cuando se cometan **por las personas encargadas o responsables de los ficheros**, soportes informáticos, electrónicos o telemáticos, archivos o registros; o se lleven a cabo **mediante la utilización no autorizada de datos personales de la víctima**, y si los datos reservados se **hubieran difundido, cedido o revelado a terceros**, se impondrán las penas en su mitad superior.

Igualmente, cuando los hechos descritos **afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección**, se impondrán las penas previstas en su mitad superior³³.

Como ha indicado MATA MARTÍN actualmente los servicios públicos (incluidos la sanidad, regulación del tráfico rodado, aéreo o marítimo, etc.) se han ido integrando inexorablemente en el entramado de las tecnologías de la información y telecomunicaciones, y junto los beneficios que proporcionan, las nuevas tecnologías engendrarían también nuevos riesgos y ocasiones para la realización de hechos ilícitos. Sobre todo, el ámbito de la privacidad de las personas se habría visto sometido a riesgos más intensos, debido a la capacidad lesiva de estos nuevos medios que permiten almacenar grandes cantidades de datos e informaciones relativas a personas, así como un

32 Asimismo se sostiene que será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, **el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior**. Cfr. igualmente sobre custodia de historia clínica, SAN JOSÉ I AMAT, “Medidas de seguridad en la custodia y gestión de las historias clínicas”, en VV.AA., *Intimidad, confidencialidad y protección de datos de salud*, Madrid, 2011, pp. 85 ss.

33 Si los hechos se realizan **con fines lucrativos**, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

tratamiento automatizado de los mismos a gran velocidad. Los procedimientos informáticos representarían desde este ángulo, la capacidad de acceso a la información, la posibilidad “de información sobre la información”³⁴.

Desde esta perspectiva, se habría reconocido la tutela de datos y las facultades atribuidas al titular de los mismos. Con la dimensión activa se afirmaría la propia libertad frente a los riesgos de la sociedad tecnológica y sería aplicable en el caso de los ficheros automatizados de datos, suponiendo la atribución de facultades de control, de posibilidades de actuación positiva, de los datos por su titular (derechos de acceso, modificación, cancelación de tales datos y de consentimiento)³⁵.

En este sentido, otros autores como PUENTE ABA habrían destacado que habría que plantearse si cualquier atentado a los datos personales recogidos en bases de datos informáticas podría constituir un delito contra la intimidad, ya que el acceso a bases de datos personales no encajaba en ninguno de los tres grupos tradicionales de conductas delictivas contra la intimidad (apoderamiento de mensajes, documentos o efectos personales; interceptación de comunicaciones; y captación del sonido o la imagen), por ello el Código penal de 1995, por primera vez, habría introducido un tipo penal específico en esta materia en el art. 197.2 CP³⁶.

En relación a cuál es el bien jurídico protegido en el tipo penal, la *Sentencia del Tribunal Supremo 1328/2009, de 30 de diciembre*³⁷, destaca que en el art. 197.2 CP se protegería la “**libertad informática o habeas data**”, es decir, el derecho a controlar el uso de los datos de carácter personal y familiar que pueden recogerse y tratarse informáticamente, con capacidad para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención.

Por lo tanto, por una parte se ampararía la intimidad del sujeto pasivo, en relación con las conductas

de apoderarse, acceder y utilizar los datos, y por otra, la integridad de los datos, en relación con los comportamientos de modificar o alterar.

El objeto material de la conducta, según esta línea jurisprudencial, sería la información de índole netamente personal, atinente a la salud del afectado, incluida y custodiada en un registro público sanitario.

Para determinar quiénes pueden considerarse como encargados o responsables de los ficheros, habría que acudir a la regulación de la Ley Orgánica de Protección de datos, donde se establece que responsable del fichero o tratamiento sería aquella “persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”; mientras que el encargado del tratamiento sería “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”³⁸.

No puede olvidarse que el artículo 197 CP contiene un tipo agravado en atención a la condición profesional del sujeto activo del delito (encargado o responsable de ficheros o bancos de datos automatizados, archivos o registros), cuyo fundamento residiría en la condición profesional del sujeto activo, que tiene acceso autorizado a los datos pero que, precisamente por ello, está especialmente llamado a velar por la reserva de éstos. Ello limita considerablemente el ámbito de aplicación del tipo cualificado, pues esa persona debe tener encomendada esa responsabilidad, otorgándole una posición de garante de discreción con respecto a los archivos y registros en los cuales constan los datos reservados³⁹.

Sin embargo, en materia de titularidad de la historia clínica existe una considerable controversia. En primer lugar, un sector doctrinal defiende que la historia clínica sería propiedad del paciente, en base a que ésta se origina en el derecho a la protección de la salud del paciente y que la mayoría de los datos que la conforman son parte de la intimidad personal de aquel. Otro sector, por el contrario, afirma que la titularidad le corresponde al médico, como propiedad intelectual del mismo, y asimismo, también se ha defendido en una tercera postura que la historia

34 MATA Y MARTÍN, “La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías”, *Revista penal*, num. 18, 2006, pp. 217 ss.

35 MATA Y MARTÍN, *ul.op.cit.*, pp. 217 ss.

36 PUENTE ABA, “Delitos contra la intimidad y nuevas tecnologías”, *EGUZKILORE* Número 21. San Sebastián Diciembre 2007 163 – 183.

37 Analiza el supuesto de un médico coordinador de Centro de Salud, que de manera subrepticia, entra en el historial médico de un colega para averiguar su médico de cabecera. En relación a la autorización se sostienen.

38 Cfr. art. 3 de la Ley orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal.

39 GOMEZ NAVAJAS, “Protección de datos personales en el Código penal español”, en *Revista Jurídica de Castilla y León*, número 16, septiembre 2008, pp. 349 ss.

clínica sería propiedad del centro sanitario en que se elabora, bien por considerarse que el mismo sería el responsable de su conservación y custodia, o bien por entenderse que la historia clínica sería el resultado de la utilización de medios materiales que el centro sanitario pone a disposición de sus profesionales⁴⁰.

En relación a posturas eclécticas al respecto, se habría considerado que cuando los datos sean relativos a la gestión y administración sanitaria, la titularidad correspondería al centro sanitario; en el caso de datos relativos a los datos personales del paciente, la titularidad sería del paciente y en el supuesto de la valoración e interpretación de la información y las pruebas clínicas, la titularidad pertenecería al médico. Asimismo, también se distingue en los casos de ejercicio individual de la medicina, cuya titularidad de la historia clínica sería compartida por el médico y el paciente, si bien éste asumiría la obligación de gestión y custodia, y los casos de ejercicio de la medicina en centros sanitarios, cuya titularidad de la historia clínica le pertenecería al centro sanitario⁴¹.

Por apoderamiento de datos reservados de carácter personal se entendería la acción de hacerse con el control de los datos de otra persona. Otra de las conductas típicas castigadas en el artículo 197.2 del CP, inciso 1.º, sería la utilización (el uso o empleo) de datos reservados (conducta prevista, asimismo, en el inciso 2.º del artículo 197.2 del CP). Se castiga, igualmente, en el primer inciso del artículo 197.2 del CP, la modificación de datos reservados, mientras que en el inciso 2.º del artículo 197.2 del CP se castiga la alteración de datos, sin que se alcance, según la doctrina, fácilmente a ver qué diferencia habría entre una y otra conducta⁴².

En relación a la clase de datos, el artículo 197.2 del CP se refiere expresamente a los datos reservados

40 GÓMEZ ÁLVAREZ, “La transmisión de datos médicos en la cooperación judicial penal y policial en el seno de la Unión Europea: en particular, la transmisión de la historia clínica”, en COLOMER HERNÁNDEZ (Director), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Cizur Menor, 2015, pp. 559 ss.

41 GÓMEZ ALVAREZ, *ul.op.cit.*, pp. 559 ss. Detalla que en relación a lo establecido por la Ley 41/2002, de 14 de noviembre, se estima que dicha normativa parte de que existe un conjunto de documentos que integran la historia clínica, y que en ellos convergen una pluralidad de derechos e intereses jurídicamente relevantes, de ahí que el legislador en lugar de resolver la cuestión de la titularidad de la historia clínica, haya optado por regular los derechos y deberes de cada una de las partes.

42 GOMEZ NAVAJAS, “Protección de datos personales en el Código penal español”, en *Revista Jurídica de Castilla y León*, número 16, septiembre 2008, pp 334 ss.

de carácter personal y familiar. La doctrina ha resalado “reservados” significar que son los datos de conocimiento limitado para terceros ajenos al fichero en el que se encuentran⁴³.

Del mismo modo, se ha sostenido que quedarían fuera del ámbito típico los datos incluidos en ficheros accesibles al público, estimándose como aquellos cuya consulta puede ser realizada por cualquier persona. Los datos incluidos en tales ficheros, por ser de acceso público para cualquier persona, ya no podrían tener la calificación de reservados⁴⁴.

En el ámbito sanitario se considera que aunque todos los datos personales automatizados, pueden ser valorados como “sensibles”, no existen, datos personales automatizados reservados y no reservados en el art. 197.2 CP, en el sentido de que no sería posible interpretar que únicamente “los datos reservados”, (“núcleo duro de la privacidad”), serían los amparados en el precepto, pero si debe exigirse en cualquier caso, que los datos o información pertenezcan al ámbito privado y personal o familiar del sujeto, siendo necesario que afecten a la intimidad personal⁴⁵.

En este aspecto, se considera que en el contenido de un historial clínico no puede tener la misma relevancia el acceso a un dato como conocer cuál sería el médico de cabecera del paciente, al conocimiento de una determinada enfermedad, máxime si es psíquica.

En lo que respecta a la tipicidad subjetiva, la *Sentencia de la Audiencia Provincial de Sevilla, número 76/2011, de 7 de diciembre*⁴⁶, estima que el elemento “en perjuicio de tercero” no supondría la exigencia de un ánimo o especial intención de perjudicar al titular de los datos o a un tercero, pues aunque el perjuicio producido por la acción tiene que estar naturalmente abarcado por el dolo, no tiene que ser el único ni el prioritario móvil de la acción; y puede considerarse que existe un perjuicio, por ejemplo, cuando los datos se usan concretamente en un proceso penal pendiente entre la persona que accede ilegalmente a los datos y su excónyuge.

43 GOMEZ NAVAJAS, *ul.op.cit.*, pp 334 ss

44 PUENTE ABA, “Delitos contra la intimidad y nuevas tecnologías”, EGUZKILORE Número 21. San Sebastián Diciembre 2007 163 – 183.

45 Cfr. *Sentencia del Tribunal Supremo 1328/2009, de 30 de diciembre*.

46 Administrativa de un hospital que obtiene la historia clínica de su exmarido aportándola en un procedimiento en el que se encontraba acusada como autora de un delito de malos tratos.

En el mismo sentido, la *Sentencia del Tribunal Supremo 40/2016*⁴⁷, de 3 de febrero, considera que en el entorno sanitario el perjuicio no sería una finalidad económica, sino que implicaría un peligro de que los datos albergados en las bases de datos protegidas pudieran llegar a ser conocidos por personas no autorizadas. El perjuicio se realizaría cuando se accede a un dato protegido con la intención de que su contenido salga del ámbito de privacidad en el que se incluyó en una base de datos especialmente protegida, no custodiada por su titular.

URRUELA MORA y ROMEO MALANDA sostienen que habría que realizar una interpretación integradora en relación a los incisos primero y segundo del art. 197.2 CP, en el sentido de que como en el inciso primero, se castigan idénticos comportamientos objetivos que el inciso 2.º (apodere, utilice, modifique) no tendría sentido que en el mero acceso no se exija perjuicio alguno y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serían punibles —y con la misma pena— en el inciso segundo. Indican que la solución sería, partiendo de que en el término “tercero” debería incluirse al afectado, en su intimidad, sujeto pasivo, considerar que los apoderamientos, accesos, utilizaciones o modificaciones de datos de carácter personal, realizadas en perjuicio de tercero se incluirían en el inciso inicial del artículo 197.2, y en cambio, en el inciso segundo deberían ser subsumidas las conductas de acceso en perjuicio del titular de los datos⁴⁸.

MATA MARTÍN afirma que en principio las conductas del 197.1 y del 197.2 CP coincidirían en la exigencia de un resultado, el apoderamiento para el inciso primero del 197.1, la interceptación o captación de la comunicación en el inciso segundo y el acceso a los datos o su modificación o utilización para los supuestos del 197.2 (al menos la conducta debe llegar al estadio de acceso a los datos). Sin embargo, señala que con base en la diferencia de objetos materiales sobre los que recae la conducta la afectación del bien jurídico tutelado sería diversa. En el ámbito del 197.1 el apoderamiento de los objetos o la interceptación de la comunicación no genera

automáticamente un conocimiento de los datos por lo que el bien jurídico únicamente ha sido amenazado o puesto en riesgo (delito de peligro), pero para el supuesto de los datos personales cuyas modalidades de ejecución deben consistir en el acceso a los mismos (o bien, en estadios más avanzados su modificación o utilización), este acceso se identificaría ya con el conocimiento del mismo dato y su contenido por lo que el bien tutelado de la intimidad informática o habeas data ha sido conculcado de manera efectiva (delito de lesión)⁴⁹.

Por tanto, considera que las conductas típicas incluirían comportamientos situados en dos segmentos distintos del ciclo total de un fichero automatizado de datos. Por una parte, se incriminan conductas realizadas sobre los datos existentes en el fichero (acceso, modificación y alteración) y, por otra, conductas posteriores cuando el dato ha sido obtenido ya del fichero (utilización). Quedarían excluidos del tipo momentos previos a la incorporación del dato al fichero (recogida ilícita de datos o formación misma del fichero)⁵⁰.

3.2. El delito de revelación de secreto laboral o profesional (art. 199 CP)

3.2.1 Elementos típicos

Como señala MUÑOZ CONDE hasta la entrada en vigor del Código penal de 1995 no se había cubierto una laguna de punibilidad existente en este campo, salvo en lo que se refería a la revelación de secretos por parte de funcionario público⁵¹.

En relación al secreto, en el art. 199 CP se contiene la conducta del que **revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales**, siendo castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

De igual modo, el **profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona**, puede ser

⁴⁷ Examina el supuesto de un médico que accede en 171 ocasiones informáticamente al historial clínico de su ex novia y al de sus familiares.

⁴⁸ URRUELA MORA, ROMEO MALANDA, “Tendencias actuales de la jurisprudencia española en materia de responsabilidad penal médica”, en <http://www.reformapenal.es/wp-content/uploads/2011/11/resmedica.pdf>, consultada en diciembre 2016, pp. 72.

⁴⁹ MATA Y MARTÍN, “La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías”, *Revista penal*, num. 18, 2006, pp. 233 ss.

⁵⁰ MATA Y MARTÍN, *ul.op.cit.*, pp. 233 ss.

⁵¹ MUÑOZ CONDE, “Falsedad documental y secreto profesional en el ámbito sanitario”, en *Derecho y Salud*, Vol.4, num.2, Julio-Diciembre, 1996, pp. 147 ss.

castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años⁵².

Se ha destacado por GÓMEZ RIVERO que el bien jurídico protegido sería la intimidad, si bien existen otros intereses que, aun cuando no lleguen a tener la consideración de bien jurídico, estarían presentes en la configuración del precepto, como la garantía de la relación de confianza, base de la relación profesional del médico con el paciente, y sin la cual sería imposible el desarrollo mismo de la actividad. Desde esta óptica quedarían fuera del precepto casos en los que un médico tuviera conocimiento de datos de un paciente que atiende otro colega, pero que él no ha tratado personalmente. Si después revelara esos datos, aunque lo hiciera con ocasión del ejercicio de su profesión, la quiebra a la intimidad habría de reconducirse, en su caso, a otros tipos delictivos, no al art. 199.2 CP⁵³.

SERRANO GONZÁLEZ DE MURILLO expone que la revelación prohibida en el tipo del art. 199.2 CP constituiría un delito de violación de secreto por parte de profesionales, entendiéndose que en el ámbito sanitario, estarían afectados por el deber de secreto profesional aquellos que para ejercer su profesión requieren un título académico oficial cuya expedición está reservada al Estado, así como la previa colegiación, y están sujetos a normas deontológicas e incluso colegiales disciplinarias: médicos, ATS/DUE, farmacéuticos, psicólogos, etc. Mientras que el resto del personal que colabore con aquéllos (medicina en equipo), sin necesidad de titulación que habilite para el ejercicio, estaría vinculado por un deber de sigilo de distinto alcance, (regulado en concreto por el art. 199.1CP, deber derivado de su oficio o de sus relaciones laborales, no de su profesión)⁵⁴.

52 En el art. 200 CP se dispone que lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

53 GÓMEZ RIVERO, *Responsabilidad médica*, Valencia, 2013, pp. 121 ss. Respecto a la exclusión del tipo penal en los casos de transmisión de datos con fines de inspección sanitaria (cita ST AP Segovia de 19 de diciembre de 2000). Cfr. Asimismo sobre el concepto de datos sanitarios, GÓMEZ RIVERO, *La protección penal de los datos sanitarios: especial consideración del secreto profesional médico*, Granada, 2007, pp. 42 ss.

54 SERRANO GONZÁLEZ DE MURILLO, “Alcance del deber de secreto del profesional sanitario ante la administración de justicia penal”, en *Revista Penal*, num.15, 2005, pp.137 ss. Cfr. Código de Deontología Médica, en CONSEJO GEN-

La *Sentencia del Tribunal Supremo, número 574/2001, de 4 de abril*⁵⁵, considera que la acción típica recogida en el art. 199.2 CP en el entorno sanitario se refiere a divulgar secretos de otra persona con incumplimiento de su obligación de sigilo, ya que tal obligación vendría impuesta por la Ley General de Sanidad 14/1986, de 25 de abril, en torno al derecho de los ciudadanos a la confidencialidad de toda la información relacionado con su proceso y con su estancia en instituciones sanitarias y concurrente en el historial clínico-sanitario, en el que deben quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica.

Por este motivo, se estima que la acción típica consiste en divulgar los secretos de una persona entendida como la acción de comunicar por cualquier medio, sin que sea necesario que se realice a una pluralidad de personas, toda vez que la lesión al bien jurídico intimidad se produciría con independencia del número de personas que tengan conocimiento⁵⁶.

Igualmente se ha indicado por la doctrina, que quedarían fuera del ámbito típico del precepto, casos como el del médico que accidental o puntualmente prestase asistencia sanitaria a una persona, ya que se exige una de actividad jurídicamente reglamentada

RAL DE COLEGIOS MÉDICOS http://www.cgcom.es/sites/default/files/codigo_deontologia_medica.pdf, cuyo artículo 27 señala: 1.□ El secreto médico es uno de los pilares en los que se fundamenta la relación médico□paciente, basada en la mutua confianza, cualquiera que sea la modalidad de su ejercicio profesional. 2.□ El secreto comporta para el médico la obligación de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, lo que haya visto y deducido como consecuencia de su trabajo y tenga relación con la salud y la intimidad del paciente, incluyendo el contenido de la historia clínica. 3.□ El hecho de ser médico no autoriza a conocer información confidencial de un paciente con el que no se tenga relación profesional. 4.□ En las instituciones sanitarias informatizadas los médicos directivos velarán por una clara separación entre la documentación clínica y la administrativa. 5.□ El médico no puede colaborar en ninguna base de datos sanitarios si no está garantizada la preservación de la confidencialidad de la información depositada en la misma. 6.□ El médico podrá cooperar en estudios epidemiológicos, económicos, de gestión, etc., con la condición expresa de que la información en ellos utilizada no permita identificar ni directa ni indirectamente, a ningún paciente. 7.□ El médico preservará en su ámbito social, laboral y familiar, la confidencialidad de los pacientes.

55 Médico que conociendo de paciente que ha interrumpido dos veces el embarazo lo comunica a tercera persona.

56 Cfr. Comentario a esta sentencia, URRUELA MORA, ROMEO MALANDA, “Tendencias actuales de la jurisprudencia española en materia de responsabilidad penal médica”, en <http://www.reformapenal.es/wp-content/uploads/2011/11/res-medica.pdf>, consultada en diciembre 2016, pp. 71 ss.

y realizada públicamente por sujetos avalados por el correspondiente título o capacitación oficial, ya que el Estado sólo puede tutelar de forma singular las actividades que reconoce y en las condiciones de legitimidad de las que hace depender en concreto su ejercicio. Asimismo también deberán excluirse del tipo a los sujetos que ejercen de forma intrusa la actividad profesional, en cuanto que, dado que realizan una función que sólo de forma aparente se orienta a la práctica de la actividad, no puede predicarse de ellos la necesidad de tutela que demanda su ejercicio⁵⁷.

En lo que respecta a los sujetos pasivos serían aquellas personas identificadas o, al menos, que resulten identificables siendo indiferente que los datos revelados se refieran al paciente o a terceros⁵⁸.

El concepto de secreto médico se extiende a la totalidad de los datos privados conocidos por el profesional en el ejercicio de su profesión (bien sea debido a la comunicación por el propio paciente o al descubrimiento por el médico en el curso de la exploración) que puedan calificarse como íntimos o reservados⁵⁹.

3.2.2 Los límites al deber de secreto en el ámbito sanitario

En lo que respecta a los datos relativos a la salud mental, GARCÍA SANZ habría sostenido que en este campo plantearía especiales problemas la cuestión de la información y el consentimiento, pues en muchos casos la persona que sufre la enfermedad puede que no se encuentre capacitada para tomar decisiones y, además, la especial vulnerabilidad en que se encuentra el enfermo supondría, en muchas ocasiones, que la información que transmite fuese más allá de lo que cualquier persona sin esos problemas desearía compartir con el médico⁶⁰.

57 GÓMEZ RIVERO, *Responsabilidad médica*, Valencia, 2013, pp. 121 ss.

58 GÓMEZ RIVERO, *ul.op.cit.*, pp.121 ss.

59 GÓMEZ RIVERO, *ul.op.cit.*, pp.121 ss, cita la STS de 4 de abril de 2001 que sostiene que “por secreto ha de entenderse lo concerniente a la intimidad, que sólo es conocido por su titular o por quien él determine”. Secretos son los datos que no son conocidos ni cognoscibles por cualquiera, y que caso de ser conocidos, pudieran resultar perjudiciales para la estima social del afectado, dificulten su vida en sociedad o simplemente revelen creencias, ideas o actitudes que se consideren estrictamente personales. Sería el caso, por ejemplo, de datos como los relativos a si la paciente se ha sometido a alguna vez a una intervención abortiva.

60 GARCÍA SANZ, “El secreto profesional en el ámbito sanitario”, en ANALES DE LA FACULTAD DE DERECHO,

Se entiende que en los casos en que el enfermo se encuentre incapacitado legalmente para dar su consentimiento, será su representante legal el que tendrá que tomar la decisión, excepto cuando el enfermo mental no estuviera enajenado hasta tal punto que no le permita consentir y pudiera ejercitar él mismo ese derecho personalísimo⁶¹.

Respecto a los límites del secreto médico⁶² en el examen de la colisión con el derecho a la información, en el caso de pacientes infectados por el virus del SIDA, **a favor del mantenimiento del secreto médico frente a la libertad de información**) el Tribunal Constitucional descartó la concurrencia de cualquier justificación a la lesión del derecho a la intimidad sobre la base de un supuesto interés superior a la información, entendiendo que la comunidad debe ser informada sobre el origen y la evolución de un determinado mal, pero ello no incluiría la individualización, directa o indirecta, de quienes lo padecen, en tanto ellos mismos no hayan permitido o facilitado tal conocimiento general⁶³.

Asimismo, también se ha defendido que el profesional quedará liberado del compromiso por *consentimiento expreso del interesado*, siempre que éste sea válidamente emitido, si bien, en estos casos se

22; diciembre 2005, pp. 187-211.,

61 GARCÍA SANZ, *ul.op.cit.*, pp. 187-211.

62 Cfr. Código de Deontología Médica, en CONSEJO GENERAL DE COLEGIOS MÉDICOS http://www.cgcom.es/sites/default/files/codigo_deontologia_medica.pdf, cuyo artículo 30 señala: 1.□ El secreto profesional debe ser la regla. No obstante, el médico podrá revelar el secreto exclusivamente, ante quien tenga que hacerlo, en sus justos límites, con el asesoramiento del Colegio si lo precisara, en los siguientes casos: a. En las enfermedades de declaración obligatoria. b. En las certificaciones de nacimiento y defunción. c. Si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo. d. Cuando se vea injustamente perjudicado por mantener el secreto

del paciente y éste permita tal situación. e. En caso de malos tratos, especialmente a niños, ancianos y

discapacitados psíquicos o actos de agresión sexual. f. Cuando sea llamado por el Colegio a testificar en materia disciplinaria. g. Aunque el paciente lo autorice, el médico procurará siempre mantener el secreto por la importancia que tiene la confianza de la sociedad en la confidencialidad profesional. h. Por imperativo legal: 1. En el parte de lesiones, que todo médico viene obligado a enviar al juez cuando asiste a un lesionado. 2. Cuando actúe como perito, inspector, médico forense, juez instructor o similar. 3. Ante el requerimiento en un proceso judicial por presunto delito, que precise de la aportación del historial médico del paciente, el médico dará a conocer al juez que éticamente está obligado a guardar el secreto profesional y procurará aportar exclusivamente los datos necesarios y ajustados al caso concreto.

63 GÓMEZ RIVERO, *Responsabilidad médica*, Valencia, 2013, pp.124 ss.

plantean problemas en cuanto a la determinación del objeto del consentimiento, pues sería el paciente el que determina con su consentimiento el campo de actuación dentro del cual podrá desenvolverse lícitamente el médico. Se indica que conforme al Código deontológico, dicha autorización no debe perjudicar la discreción del médico, que procurará siempre mantener la confianza social hacia su confidencialidad⁶⁴.

En lo relativo a enfermedades contagiosas, se afirma que la protección penal no podría ceder incondicionalmente ante un supuesto interés de mayor calado que, con carácter general, actuase cancelándola. Se considera que no existiría una obligación genérica del profesional de revelar los datos que conoce cuando peligre en abstracto la vida o la salud de terceras personas. Ni siquiera pudiera exigírsele al médico un deber de asegurarse y de velar para que efectivamente el paciente tome las medidas oportunas tendentes a evitar el contagio, sino que al contrario, sería lícito que aquél se limitara a confiar en que, una vez advertido, el enfermo adoptará de *motu proprio* las precauciones pertinentes⁶⁵.

GÓMEZ RIVERO sostiene que la revelación de los datos en el caso concreto requerirá comprobar **la concurrencia de los presupuestos de un estado de necesidad**, es decir, que la lesión del interés que se contrapone a la intimidad no se plantee en términos meramente genéricos o potenciales, sino que se encuentre, *de facto*, en una situación de peligro actual e inminente. Por ello, cuando ese otro interés que se contrapone a la intimidad del paciente sea la vida o salud de terceros, para que prevalezcan sobre la intimidad habrá de tratarse de supuestos en los que, por una parte, concurren circunstancias que hagan sospechar que el paciente pueda convertirse en una fuente de peligro grave para terceros y, por otra, existan razones fundadas para pensar que su evitación no pueda confiarse a la adopción de medidas protectoras por parte de aquél. Como regla general, la primacía del derecho a la intimidad habrá de mantenerse en todos aquellos casos en los que el interés a ella contrapuesto no se traduzca en la evitación de un riesgo para la vida o salud de las personas o no se implique con intereses de carácter general⁶⁶.

GARCÍA SANZ habría sostenido que en relación a los datos genéticos en aquellos casos en que la información revela datos no sólo del enfermo, sino también de sus familiares biológicos por el denominado “*carácter familiar de la información genética*”, los perjuicios se pueden extender a una persona que no ha consentido someterse a la prueba. En estos casos se cuestionaría si el descubrimiento de una enfermedad genética hereditaria, obliga a comunicar al resto de la familia dicho extremo, pues si bien se debe proceder con extrema cautela (no existe la obligación de transmitir el hallazgo y, además, se debe respetar el derecho de los familiares a “no saber”) **la posible existencia de un grave riesgo para terceros limitaría la confidencialidad** en los casos que sea necesario para evitar el grave daño en sus familiares, entendiéndose que si bien el principio de autodeterminación implica también un derecho a “no conocer”, este *derecho* debe ceder en aquellos casos que se encuentre en peligro la vida o salud de los mismos⁶⁷.

En materia de declaraciones periciales o testificales MUÑOZ CONDE habría expuesto que hay que partir del **derecho del médico a no tener obligación de testificar ni de realizar informe pericial** revelando datos que conoce del paciente en su correspondiente ejercicio profesional, sobre todo en aquellos casos en los que el sanitario conoce las implicaciones en hechos delictivos referidos al pasado. Sin embargo, ello no sería predicable en los casos de hechos delictivos futuros, que pudieran ser evitables y donde se conculquen derechos fundamentales de otras terceras personas⁶⁸.

3.2.3 El tratamiento penal del error en el ámbito de la intromisión ilegal y revelación de datos clínicos

En lo que se refiere al tratamiento del error de prohibición indirecto en estos casos, la *Sentencia del Tribunal Supremo 778/2013, de 22 de octubre*, analiza un supuesto en el que un cirujano investigó documentación de pacientes suyos y de otros médicos, al

2013, pp.124 ss.

64 GARCÍA SANZ, *ul.op.cit.*, pp. 187-211. ROMEO CASABONA, C., *La protección penal del secreto profesional y laboral en el Derecho penal*, Estudios penales en recuerdo del Profesor

Ruiz Antón, Valencia, 2004, págs. 977 y 979.

65 GÓMEZ RIVERO, *Responsabilidad médica*, Valencia, 2013, pp.124 ss.

66 GÓMEZ RIVERO, *Responsabilidad médica*, Valencia,

67 GARCÍA SANZ, “El secreto profesional en el ámbito sanitario”, en ANALES DE LA FACULTAD DE DERECHO, 22; diciembre 2005, pp. 187-211.

68 MUÑOZ CONDE, “Falsedad documental y secreto profesional en el ámbito sanitario”, en *Derecho y Salud*, Vol.4, num.2, Julio-Diciembre, 1996, pp. 147 ss. Cfr. igualmente ampliamente sobre el secreto profesional en el campo de la medicina, abogacía y profesionales de la información, MUÑOZ CONDE, *Derecho penal, Parte especial*, Valencia, 2015, pp. 264 ss.

detectar un posible problema sanitario en las prótesis mamarias implantadas en la clínica a la que pertenecía.

Se estima por el Tribunal Supremo que en relación al art. 199 CP (secreto profesional) la conducta estaría justificada por el cumplimiento de un deber, ya que poner los hechos en conocimiento de la fiscalía no sería revelar secretos, sino cumplir con la obligación impuesta con especial intensidad al médico.

Sin embargo, en lo que respecta a acceder a los datos de personas que no eran pacientes suyas y la comisión de un delito contra la intimidad previsto art. 197.2 CP, se considera la existencia de un error de prohibición invencible al valorar que dicho cirujano creyó, razonablemente, que existía un peligro para la salud de pacientes intervenidas en la Clínica, que se había cometido un delito de estafa y otro contra los derechos de los consumidores, de los que él mismo podría ser responsable por su intervención profesional. Se considera acreditada la invencibilidad del error ante las circunstancias de que dicho médico se había asesorado previamente jurídicamente con profesionales del Derecho, actuando en la creencia, errónea, de que la denuncia que formulaba, requería una previa indagación de los hechos.

Asimismo, en materia de error de prohibición sobre los presupuestos objetivos de una causa de justificación como el estado de necesidad, la *Sentencia del Tribunal Supremo número 990/2012, de 18 de octubre*, enjuició el caso de una enfermera que accedió al archivo clínico de la nueva pareja de su excuñado, aduciendo que la enfermedad psíquica de aquella podía perjudicar a sus sobrinos, poniendo en conocimiento de su hermana la información obtenida y siendo esta información utilizada en un procedimiento matrimonial.

El Tribunal Supremo expone que no cabría apreciar ni estado de necesidad ni error de prohibición en este supuesto, ya que la creencia no podría apoyarse ni en Códigos Deontológicos de la profesión, ni en la salvaguarda de los derechos de los menores, ya que solo se permitiría violar la confidencialidad cuando el silencio pudiera suponer un grave peligro colectivo, para el paciente o para terceros.

Se detalla que no puede excluirse la responsabilidad penal en aquellos casos en los que el sujeto actúa a título exclusivamente privado, y no como profesional de la enfermería. La norma deontológica guardaría relación con el deber de denunciar una posible infracción o peligro observados por un profesional en

el ejercicio de su actividad, pero no otorga la facultad de disponer de datos reservados para su cesión a un tercero, a fin de que los utilizara en el seno de un procedimiento matrimonial de carácter privado.

IV. CONCLUSIONES

Conforme a la normativa de protección de datos de la Unión Europea, tras las modificaciones introducidas durante el 2016, podemos considerar datos sanitarios a todos aquellos datos personales relacionados con la salud, física o mental pasada, presente o futura, incluidos los datos personales recopilados durante la inscripción de una persona física a efectos de la prestación de servicios de asistencia sanitaria, identificándola de manera unívoca, la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, (incluidos los datos genéticos y las muestras biológicas), y cualquier información relativa a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, ya sea un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

En relación a la comisión de delitos contra la intimidad de las personas, puede estimarse que en esta materia, en el art. 197.2 CP, en relación al descubrimiento de datos reservados recogidos en archivos o registros, se protegería la “*libertad informática o habeas data*”, es decir, el derecho a controlar el uso de los datos de carácter personal y familiar que pueden recogerse y tratarse informáticamente, con capacidad para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención.

Por otra parte, respecto a qué clase de datos sanitarios se protegerían penalmente, se ha destacado que no podría interpretarse que “los datos reservados” recogidos en el tipo penal serían únicamente los más sensibles, (“núcleo duro de la privacidad”), pero sí deberá exigirse en cualquier caso, que los datos o información pertenezcan al ámbito privado y personal o familiar del sujeto, siendo necesario que afecten a la intimidad personal.

En lo concerniente a que la utilización de estos datos sanitarios se produzca en perjuicio del titular de los datos o de un tercero, se considera que dicho perjuicio no tiene por qué tener una finalidad

exclusivamente económica, sino que dicho perjuicio se concretaría cuando el sujeto activo accede, a sabiendas, a un dato protegido con la intención de que su contenido salga del ámbito de privacidad en el que se incluyó en una base de datos especialmente protegido, no custodiado por su titular, como puede suceder en aquellos casos, en los que dichos datos se usan en contra del sujeto pasivo en procesos judiciales pendientes contra los mismos.

En torno al examen de la existencia y límites de un error de prohibición indirecto, creyendo obrar el autor al amparo de un estado de necesidad, se ha estimado que cuando el sanitario accede ilegalmente a los datos, la norma deontológica sanitaria se basaría en el deber de denunciar una posible infracción o peligro observados por un profesional en el ejercicio de su actividad, pero ello no otorgaría la facultad de disponer por el propio sanitario de datos reservados para su cesión a un tercero, a fin de que los utilice en el seno de un procedimiento de carácter privado.

Igualmente, respecto al delito de quebrantamiento del secreto profesional, en relación al concepto de secreto médico entendemos, asimismo, que éste abarcaría al conjunto de datos privados conocidos por el profesional en el ejercicio de su profesión, siempre que éstos puedan calificarse como íntimos o reservados. Por ello, se cometería el delito previsto en el art. 199.2 CP en aquellos casos en los que el profesional sanitario, *obligado al deber de sigilo*, divulgase secretos de otra persona, conculcándose el derecho de los pacientes a la confidencialidad de toda la información ligada a su proceso y su estancia en centros sanitarios, así como la registrada en el historial clínico, no respetándose el derecho del enfermo a su intimidad personal y familiar.

V. BIBLIOGRAFÍA

- ANDREU MARTÍNEZ, ALARCÓN SEVILLA, SALCEDO HERNÁNDEZ, SORO MATEO, “Sanidad electrónica e intercambio de información sanitaria en Europa a la luz de la nueva regulación sobre protección de datos personales”, en *Derecho y Salud*, Vol. 24 Extraordinario XXIII Congreso 2014.
- FERNÁNDEZ PANTOJA, “El delito de revelación de secretos en el ámbito sanitario”, en <http://libros-revistas-derecho.vlex.es/vid/oacute-secretos-mbito-sanitario-219796997>, pp. 287-321, consultada en diciembre 2016.
- GARCÍA SANZ, “El secreto profesional en el ámbito sanitario”, en ANALES DE LA FACULTAD DE DERECHO, 22; diciembre 2005. [http://publica.webs.ull.es/upload/REV-ANALES/22-2005/12 \(Judit García Sanz\).pdf](http://publica.webs.ull.es/upload/REV-ANALES/22-2005/12%20(Judit%20García%20Sanz).pdf)
- GARRIGA DOMINGUEZ (Dirección), “Historia clínica y protección de datos personales: recomendaciones y propuestas en torno al uso de la información”, *Informe elaborado en el marco del laboratorio de la sociedad de la información y derechos humanos dentro del programa “el tiempo de los derechos”, consolidar-ingenio 2010, por el Grupo de investigación HI13 de la Universidad de Vigo, noviembre 2010.*
- GÓMEZ ÁLVAREZ, “La transmisión de datos médicos en la cooperación judicial penal y policial en el seno de la Unión Europea: en particular, la transmisión de la historia clínica”, en COLOMER HERNÁNDEZ (Director), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Cizur Menor, 2015.
- GOMEZ NAVAJAS, “Protección de datos personales en el Código penal español”, en *Revista Jurídica de Castilla y León*, número 16, septiembre 2008.
- GÓMEZ RIVERO, *Responsabilidad médica*, Tirant Lo Blanch, Valencia, 2013.
- GÓMEZ RIVERO, *La protección penal de los datos sanitarios: especial consideración del secreto profesional médico*, Comares, Granada, 2007.
- GONZÁLEZ GARCÍA, “El derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos”, *Derecho y salud*, vol.24, 2014.
- MATA Y MARTÍN, “La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías”, *Revista penal*, num. 18, 2006.
- MUÑOZ CONDE, *Derecho penal, Parte especial*, Tirant Lo Blanch, Valencia, 2015.
- MUÑOZ CONDE, “Falsedad documental y secreto profesional en el ámbito sanitario”, en *Derecho y Salud*, Vol.4, num.2, Julio-Diciembre, 1996.
- PUENTE ABA, “Delitos contra la intimidad

y nuevas tecnologías”, EGUZKILORE Número 21. San Sebastián Diciembre 2007 163 – 183.

- ROMEO CASABONA, *La protección penal del secreto profesional y laboral en el Derecho penal*, Estudios penales en recuerdo del Profesor Ruiz Antón, Tirant Lo Blanch, Valencia, 2004.

- ROMEO CASABONA, “El tratamiento y la protección de los datos genéticos”, *Gen-Ética.*, Barcelona 2003.

- ROMEO CASABONA, (Coordinación), *El Convenio de Derechos Humanos y Biomedicina. Su entrada en vigor en el ordenamiento jurídico español*, Comares, Bilbao-Granada 2002.

- ROMEO CASABONA, “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, julio-diciembre, 1993.

- SAN JOSÉ I AMAT, “Medidas de seguridad en la custodia y gestión de las historias clínicas”, en VV.AA, *Intimidad, confidencialidad y protección de datos de salud*, Madrid, 2011.

- SÁNCHEZ CARO, ABELLÁN, *Datos de salud y datos genéticos. Su protección en la Unión Europea y en España*, Comares, Granada, 2004.

- SERRANO GONZÁLEZ DE MURILLO, “Alcance del deber de secreto del profesional sanitario ante la administración de justicia penal”, en *Revista Penal*, num.15, 2005.

- SERRANO PÉREZ, “La protección de los datos sanitarios en Europa. La historia clínica”, en https://www.uclm.es/actividades0506/seminarios/proteccion_datos/pdf/datos_sanitarios.pdf, consultada en junio 2016.

- URRUELA MORA, ROMEO MALANDA, “Tendencias actuales de la jurisprudencia española en materia de responsabilidad penal médica”, en <http://www.reformapenal.es/wp-content/uploads/2011/11/resmedica.pdf>, consultada en diciembre 2016.