¿TIENE EL PACIENTE DERECHO A SABER QUIÉNES Y POR QUÉ HAN ACCEDIDO A SU HISTORIA CLÍNICA?

Sergio Gallego Riestra

Coordinador de Responsabilidad Patrimonial y Régimen Disciplinario de la Consejería de Sanidad del Principado de Asturias. Presidente de la Comisión Asesora de Bioética del Principado de Asturias.

Isolina Riaño Galán

Jefa del Servicio de Pediatría del Hospital San Agustín de Avilés. Vocal de la Comisión Asesora de Bioética del Principado de Asturias.

ÍNDICE

RESUMEN

Se plantea si el paciente tiene derecho o no a conocer quiénes han accedido a su historia clínica como una forma de garantizar su derecho a la protección de datos y a la intimidad. La AEPD, el Ministerio de Sanidad y alguna norma autonómica sostienen que no existe tal derecho, lo que sin duda conducirá a una mayor judicialización de las relaciones de los ciudadanos con el sistema sanitario

PALABRAS CLAVE

Intimidad, protección de datos, historia clínica, registro de accesos..

ABSTRACT

Arises whether the patient is entitled or not to know who has accessed his medical history as a way to guarantee his right to data protection and privacy. Non-recognition of this right will lead to greater judicialization relation between citizens and the health system.

KEYWORDS

Privacy, data protection, medical history, access log

1. INTRODUCCIÓN

Si yo fuera el Gerente de un hospital, cada vez que una persona famosa ingresase en él pediría al Servicio de Documentación Clínica que me diese el listado de todo el personal que hubiese accedido in-

debidamente a su historia clínica. Después les citaría en mi despacho y les preguntaría los motivos de su conducta, para, a continuación, iniciar las medidas sancionadoras pertinentes contra todos aquellos que no tuviesen una justificación legal que la amparase.

Si yo fuese una persona famosa, cada vez que ingresase en un hospital exigiría que me proporcionasen el listado de todos los trabajadores que hubieran accedido a mi historia clínica. Pero probablemente no me lo darían y entonces encomendaría a mis abogados que se encargasen del asunto. Casi con seguridad, lo primero que harían sería poner una querella contra el Gerente, el Director Médico y todos aquellos que, en un grado u otro de autoría, pudiesen estar inmersos en la presunta comisión de un delito de descubrimiento de secretos. Sólo así, como una prueba pedida a través del juez dentro de una causa criminal, podría obtener el listado de accesos que las organizaciones sanitarias se niegan frecuentemente a dar en base a una restrictiva interpretación de la normativa vigente que viene siendo amparada por la Agencia Española de Protección de Datos (AEPD).

Esta podría ser la base para una noticia, con indudable interés periodístico, sobre una incongruente y sorprendente situación que se está produciendo en nuestro país en relación con el derecho de los pacientes a controlar y conocer quiénes acceden a sus historiales clínicos.

La interpretación que vienen realizando los tribunales de justicia de las normas sobre protección de datos personales es absolutamente amplia y garantista a favor de su titular. Así, el Tribunal Constitucional señala que la llamada "libertad informática" es el derecho a controlar el uso de los datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención. [1]

El mismo tribunal matiza que "El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidos de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin".

La sentencia, añade "En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele"[2].

En sintonía con esta doctrina constitucional, la sentencia de la Audiencia Nacional de 2 de febrero de 2005**,** dice que la protección de datos tiene como contenido esencial el conferir a la persona afectada el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera intima de la persona y la prohibición de usar los datos a ella referentes.

2.- NORMATIVA GENERAL EN MATERIA DE PROTECCIÓN DE DATOS

Por razones obvias de espacio, nos referiremos de manera muy escueta nada más que a aquellos preceptos que regulan exclusivamente las cuestiones que son objeto del presente estudio.

2.1 La obligación de elaborar y conservar un registro de accesos a la historia clínica que identifique a cada usuario que entre en ella o lo intente

El **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, establece que t**odos los ficheros o tratamientos de datos de carácter personal deberán adoptar unas medidas de seguridad que se clasifican en tres niveles: básí-

1 Sentencia Tribunal Constitucional 11/1998 de 13 de enero.

2 Sentencia Tribunal Constitucional 292/2000, de 30 de noviembre.

co, medio y alto. En el art. 81.3 señala que, además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán, entre otros, a los ficheros o tratamientos que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

Por tanto, todos los ficheros en los que se contengan datos relativos a las salud, es decir, las historias clínicas cualquiera que sea el tipo de soporte en el que se encuentren, están sometidos al nivel máximo se seguridad. Ello implica, entre otras cosas y a los únicos efectos que ahora nos interesan, que el responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios y establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. Además, y como fruto del alto nivel de seguridad que corresponde, resulta aplicable el artículo 103 del Real Decreto que literalmente dice que 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.

Si este tipo de archivos no estuviera automatizado, como es el caso de las historias clínicas en soporte papel, **la misma norma impone que** el acceso a la documentación se limite exclusivamente al personal autorizado y que se establezcan mecanismos que permitan identificar los accesos realizados debiendo quedar adecuadamente registrados.

En este momento ya podemos extraer una primera conclusión. Cada acceso o intento de acceso a la historia clínica obliga a que quede identificado inequívoca y personalmente el usuario, entendiendo por tal, todas las personas que acceden a ella. De cada 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. Este registro de accesos se conservará al menos durante dos años.

2.2 El derecho de acceso del interesado a los datos incluidos en un fichero o sometidos a tratamiento

La normativa en materia de protección de datos reconoce al titular de los mismos el derecho de acceso a sus propios datos. Así, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, cuando regula los derechos de los ciudadanos en relación con sus datos hace especial referencia al derecho de acceso. En su artículo 15.1 dispone que "El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos".

En cuanto al concepto legal de comunicación o cesión de datos, el artículo 3 i) de la Ley indica que es "toda revelación de datos realizada a una persona distinta del interesado".

La Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, define la cesión como la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los datos, su cotejo o interconexión.

El **Reglamento de desarrollo de la Ley Orgánica 15/1999 establece en el artículo 27 que "**El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. 2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento".

En el artículo 29 regula cómo se otorga al interesado el derecho de acceso: "3. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos".

3.- NORMATIVA ESPECÍFICA EN RELACIÓN CON LA HISTORIA CLÍNICA

Como ya hemos comentado antes, nos ceñiremos tan sólo a la regulación relacionada con nuestros objetivos en este momento.

3.1 Quiénes están legitimados para acceder a la historia clínica

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 establece en el artículo 16 los usos de la misma y en función de ellos determina quiénes pueden acceder a ella. De manera muy resumida podemos decir que los accesos regulados son los siguientes:

- Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente pueden acceder a la historia clínica para garantizar una asistencia adecuada al paciente.

- El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, puede acceder a la historia clínica en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

- El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

- El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de 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. Tan solo se exceptúan de este acceso anonimizado los supuestos de investigación de la autoridad judicial y de prevención de un riesgo o peligro grave para la salud de la población.[3]

Cualquier acceso diferente a los mencionados será un acceso no amparado por la Ley y por tanto un acceso ilegal. En este momento es preciso recordar que el artículo 7 de la misma Ley 41/2002 determina que, a fin de proteger su intimidad, toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley; imponiendo a los centros sanitarios la obligación de adoptar las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y de elaborar, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes.

3.2 El derecho de acceso del paciente a su historia clínica. Su alcance y límites. La normativa básica. Referencia a algunas normas autonómicas

En el artículo 18 de la Ley 41/2002 se regula el derecho de acceso a la historia por parte del paciente o, en caso de fallecimiento, de las personas a él vinculadas por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite**. Señala que e**l paciente tiene el derecho de acceso a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella.

Como límites, la Ley sólo establece que el derecho al acceso del paciente a la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

Además de la normativa estatal, varias normas autonómicas se han ocupado de la regulación de la historia clínica. Las dos que ahora mismo centran nuestro interés son la de Galicia y la de Castilla La Mancha, dado que se ocupan de manera específica de la historia en soporte electrónico o digital y de los registros de accesos a las mismas.

El Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica en Galicia introduce como interesantísima novedad el posible establecimiento, dentro de la historia, de módulos de especial custodia a petición del paciente. En ellos se contendrían datos e información clínica que puedan afectar especialmente a su intimidad. Se

3 Según la redacción introducida por la Ley 33/2011, de 4 de octubre, General de Salud Pública.

pretende, como idea general, ocultar su existencia a los demás profesionales que entren en la historia, pero dejando la puerta abierta a que, de manera motivada, se pueda acceder a ellos. En este caso, la aplicación informática dejará constancia de este hecho, de tal manera que en "el registro de accesos quedarán singularizados los correspondientes a los datos de especial custodia, lo que permitirá realizar auditorías específicas".

Es decir, la norma gallega, en la práctica, prevé la creación de dos registros de accesos a la historia clínica. El habitual que viene impuesto por la normativa estatal en materia de protección de datos y otro específico de los accesos efectuados por los profesionales a los módulos de especial custodia.

Por su parte el Decreto 24/2011, de 12 de abril, de la documentación sanitaria en Castilla-La Mancha, se ocupa del control de los accesos a la historia por parte de los profesionales en los siguientes términos. Comienza señalando que los sistemas de información de la historia clínica electrónica identificarán de forma inequívoca y personalizada a todo profesional que acceda o intente acceder a la información contenida en la historia clínica electrónica y verificarán su autorización. Se guardarán, como mínimo, la identificación del profesional de que se trate, la fecha y hora en que se realizó, la parte de la historia clínica electrónica a la que se ha accedido y el tipo de acceso.

Cuando regula el derecho de acceso del paciente a su historia clínica sigue lo establecido en la Ley 41/2002 de autonomía, pero añadiendo como novedad lo previsto en **Reglamento de desarrollo de la Ley Orgánica 15/1999:**

Artículo 19. Extensión del derecho de acceso.-

1. El paciente tiene derecho de acceso a la información contenida en la historia clínica y a obtener copia de los informes o datos que figuran en la misma. Este derecho comprende, asimismo, la posibilidad del paciente de obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas sobre los mismos.

2. 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.

Este último párrafo, ajeno a cualquier norma jurídica previa, manifiesta expresa e inequívocamente que el paciente no tiene derecho a saber quiénes han podido acceder a su historia. Su redacción no es del todo clara. ¿Cuando menciona "los datos personales" de aquéllos que hayan accedido a la historia se refiere incluso a su mera identificación personal? Está claro que sí. Dato personal, según el artículo 3.a) de la Ley Orgánica15/1999 es "cualquier información concerniente a personas físicas identificadas o identificables". Por añadidura, el artículo 5. 1 f) del Real Decreto 1720/2007, considera dato de carácter personal a "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

3.3.- La Historia Clínica Digital del Sistema Nacional de Salud

En la página web del Ministerio de Sanidad, Servicios Sociales e Igualdad se encuentra el denominado **Sistema de Historia Clínica Digital del Sistema Nacional de Salud[4]. Su implantación se encuentra en estos momentos en fase de prueba en diferentes Comunidades Autónomas. Es un extenso documento en el que se explica el diseño efectuado por el Ministerio para establecer una historia clínica compartida que** posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, a fin de evitar la repetición innecesaria de exploraciones y procedimientos.

Centrándonos exclusivamente en el objeto de este artículo, es decir, en el alcance del derecho de acceso de los ciudadanos a sus historiales clínicos, hay que destacar que de forma explícita lo recoge en el punto 3, donde afirma que para los ciudadanos el sistema ofrece tres tipos de funcionalidades:

- Acceso a los conjuntos de datos personales sobre su salud

- Acceso al registro de accesos producidos a sus conjuntos de datos

4 http://www.msps.es/profesionales/hcdsns/home.htm

• La posibilidad de ocultar aquellos conjuntos de datos que no deben ser conocidos por profesionales distintos de quienes habitualmente le atienden.

En cuanto al segundo punto, literalmente afirma: "El ciudadano puede realizar el seguimiento de los detalles de los accesos realizados desde este sistema a sus propios conjuntos de datos, a fin de poder verificar la legitimidad de los mismos. Dispondrá para ello de información relativa al momento en que se realizó el acceso, Servicio de Salud, centro sanitario y servicio desde el que se realizó cada acceso, así como las características del documento electrónico accedido. Cada vez que un ciudadano haga uso de esta funcionalidad ejercerá como auditor externo del sistema, (…)". Expresamente señala que esta información se proporciona para que cada ciudadano pueda llevar a cabo el control de su derecho a la confidencialidad.

4.- LA INTERPRETACIÓN DE LA AEPD RESPECTO AL DERECHO DE ACCESO AL "REGISTRO DE ACCESOS"

Como indudable origen de estas interpretaciones restrictivas de las normas sobre protección de datos, se encuentra el criterio reiteradamente manifestado por la AEPD. En sus informes jurídicos y en sus resoluciones expresa de manera inequívoca que los pacientes no tienen derecho a conocer quiénes han accedido a sus historiales médicos.

Resulta meridianamente claro y explícito el Informe Jurídico 171/2008. Un centro sanitario consulta si debe acceder a la petición realizada por una persona que pretende que se le proporcionen los datos de los trabajadores del centro que hubieran asistido a las personas a las que las historias clínicas se refieren. La AEPD contesta literalmente: "debe considerarse que el conocimiento de los concretos usuarios de la organización que hubieran accedido a los datos de carácter personal de la historia clínica no puede en ningún caso entenderse comprendido dentro del derecho de acceso a tribuido al afectado por la Ley Orgánica 15/1999, como ha tenido la ocasión de indicar esta Agencia Española de Protección de Datos en reiteradas resoluciones, (…). Por tanto, la revelación de los datos de los facultativos o personal que atendió a las afectadas no se encontrará amparada por el ejercicio del derecho de acceso, no procediendo otorgar el mismo en relación con este punto (…)".

En los mismos términos se pronuncia la Resolución R/02036/2010 de 7 de octubre de 2010 (Procedimiento TD/01057/2010). La interesada había solicitado a un centro hospitalario "los datos de las personas que hubiesen accedido a su historia clínica electrónica". El hospital le niega la petición hecha, motivo por el cual presenta ante la Agencia de Protección de Datos una reclamación al entender que no ha sido atendido su derecho de acceso. La Resolución inadmite la reclamación esgrimiendo como única argumentación que "conforme a la LOPD el reclamante sólo puede solicitar sus propios datos personales, o los de aquellas personas cuya representación ostente".

Idéntico criterio sostiene la Agencia de Protección de Datos de la Comunidad de Madrid cuando señala "En ningún caso constituyen datos de carácter personal, ni cesiones de datos realizadas, los accesos que los usuarios de la historia clínica, en el ejercicio de la actividad asistencial, hayan realizado a la misma. El criterio manifestado por esta Agencia en informes anteriores ha sido siempre que no se deben facilitar al solicitante del ejercicio del derecho de acceso el seguimiento de los accesos realizados a los ficheros en los que se encuentren sus datos de carácter personal".[5]

A pesar de la rotundidad de estos informes merece la pena hacer una matización. La Agencia madrileña afirma que los accesos realizados por los trabajadores en el ejercicio de la actividad asistencial no son cesiones de datos. En clara contradicción con esta afirmación, la AEPD, en el informe jurídico 171/2008 antes citado señala que los artículos 16 y 18 de la Ley 41/2002 de autonomía del paciente, regulan los supuestos en que se podrá producir la cesión de datos de la historia clínica, así como el modo en que podrá producirse el acceso a la misma. Respecto de las cesiones, dice la Agencia que el artículo 16 dispone 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. No sabemos si de manera consciente o no, la AEPD no duda en calificar el acceso por los profesionales como cesión y sin embargo, unas líneas después niega el derecho de los usuarios a conocer quiénes han accedido a sus historiales, cuando la regulación del derecho de acceso incluye literalmente el derecho a conocer quienes

5 "Contenido del ejercicio del derecho de acceso por parte de una paciente a su historia clínica". Revista digital datos personales.org de la Agencia de Protección de Datos de la Comunidad de Madrid, nº 50 11 de abril de 2011

son los cesionarios de los datos.

Ahora bien, quizá lo más sorprendente es que el solicitante lo que pretendía en este caso, era, además del acceso al contenido de unas historias, que se le proporcionasen los datos identificativos de los facultativos y personal que hubieran tratado a las pacientes. Es la propia AEPD la que afirma que "los datos a los que se refiere la consulta serían los relativos a los usuarios que hubieran accedido a los datos personales contenidos en la historia clínica". Es decir, considera que quienes trataron a las pacientes son los mismos que accedieron a sus historias. Pues si esa es la interpretación sorprende aún más la negativa a proporcionar la información pedida, ya que se trata de un derecho expresamente reconocido por Ley.

En este sentido, la Ley 44/2003, de 21 de noviembre, de Ordenación de las profesiones sanitarias, en el artículo 5.1, e) dice. "Los profesionales y los responsables de los centros sanitarios facilitarán a sus pacientes el ejercicio del derecho a conocer el nombre, la titulación y la especialidad de los profesionales sanitarios que les atienden, así como a conocer la categoría y función de éstos, si así estuvieran definidas en su centro o institución".

5.- CONFIGURACIÓN ACTUAL DEL DELITO DE DESCUBRIMIENTO DE SECRETOS AJENOS EN EL CÓDIGO PENAL

El Código Penal dedica el Capítulo I del Título X a los delitos de descubrimiento y revelación de secretos, configurándolos bajo varias formas de comisión. Así, en el artículo 197.2 se encuentra tipificada como delito la conducta de quien sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen 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.

En este último párrafo se ha visto, tanto por la doctrina como por la jurisprudencia, la penalización del acceso indebido a la Historia Clínica.[6]

Fruto de la reforma del Código Penal realizada en 2010 es la redacción del punto 3 del mismo artículo: "El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".[7]

El apartado 4 del artículo 197 establece que "Se impondrá 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 a que se refieren los números anteriores". Esta sería la figura delictiva de divulgación de secretos ajenos, diferente sustancialmente de la de descubrimiento que no exige divulgación de dato alguno y se consuma por el mero acceso cuando no tiene amparo legal.[8]

Finalmente, el Código (Art.197.6) establece como una forma agravada la comisión de estos delitos cuando los hechos descritos en los apartados anteriores 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 un incapaz, en cuyo caso se impondrán las penas previstas en su mitad superior.

Este artículo ha dado lugar a algunas sentencias condenatorias en casos directamente relacionados con datos de salud. En un primer caso el condenado es un periodista que accedió, en opinión del Tribunal, de forma ilícita a los registros informáticos de un centro penitenciario y difundió, posteriormente, que dos reclusos enfermos de sida estaban destinados en la cocina. La sentencia considera que aunque no dio datos que permitiesen su identificación, el delito de descubrimiento se consuma tan pronto como el sujeto activo accede a los datos, esto es, tan pronto como los conoce y tiene a su disposición, pues sólo con eso se quiebra la reserva que los cubre.[9]

6 GALLEGO RIESTRA, Sergio "Responsabilidad profesional y Gestión de Riesgos". en Díaz de Santos (José Mª Antequera Vinagre): *Derecho y Sociedad. Dirección Médica y Gestión Clínica*. 2006, pag. 99-172. SÁNCHEZ CARO, Javier, SÁNCHEZ CARO, Jesús: *El Médico y la Intimidad,* Díaz de Santos. Madrid 2001, pag 116

7 Redacción según Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

8 GALLEGO RIESTRA Sergio, BOBES GARCÍA Julio. *Últimas tendencias de la responsabilidad profesional médica con especial atención a la intimidad*; Grupo Ars XXI de Comunicación, S.L. Barcelona (España). 2006, pag. 37

9 Sentencia del Tribunal Supremo 234/1999, de 18 de febrero de 1999

También tiene especial interés la Sentencia de la Audiencia Provincial de Palma de Mallorca nº 11/2009, de 11 de febrero de 2009, que pone de manifiesto la severidad de las penas que impone el Código Penal para estos delitos. Un médico accedió a la historia clínica de otro médico, que a la vez también era paciente del mismo centro. El médico que realizó el acceso mantenía que lo hizo exclusivamente para conocer el nombre del médico de cabecera de su compañero, pero la Audiencia, a pesar de ello, le condena como autor de un delito continuado de acceso a datos reservados de carácter personal a las penas de 3 años y 3 meses de prisión, multa de 21 meses, con una cuota diaria de 6€, e inhabilitación absoluta por un periodo de 9 años.

Esta Sentencia ha sido casada por el Tribunal Supremo mediante la Sentencia núm. 1328/2009 de 30 diciembre, por la que absuelve al médico coordinador. El Tribunal considera que sólo ha quedado probado que accedió al nombre del médico de cabecera del paciente y no considera que se trate de un dato sensible, calificándolo de dato administrativo, y en principio, inocuo. Así todo, lo que es relevante es el criterio judicial de que el acceso indebido a la historia clínica es constitutivo de un delito de descubrimiento de secretos al que cabe aplicar las formas agravadas al tratarse de datos de carácter personal relativos a la salud. En este caso concreto, lo que ha entendido el Tribunal Supremo es que efectivamente no se produjo el acceso a esos datos de salud que son los realmente sensibles.

Además de estas sentencias comentadas, hemos tenido oportunidad de ver otros pronunciamientos judiciales y administrativos que condenan expresamente el acceso indebido a la historia clínica.[10]

Existe un último hecho absolutamente trascendente para nuestro estudio. El Código Penal establece que para perseguir estos delitos es necesario que exista denuncia de la persona agraviada o de su representante legal, salvo que el autor fuera autoridad o funcionario público.

10 Sentencia núm. 70/2009 de 23 marzo del Tribunal Constitucional (Sala Primera). STSJ Extremadura 1932/2002 de 25 de noviembre (Jurisdicción: Contencioso-Administrativa). Sentencia núm. 467/2009 de 4 noviembre de la Audiencia Provincial de Las Palmas (Jurisdicción Civil). Sentencia núm. 507/2011 de 4 octubre de la Audiencia Provincial de Valencia (Jurisdicción Penal) y Dictamen 188/2008 del Consejo de Estado.

6.- EL DERECHO DE ACCESO A LOS REGISTROS Y ARCHIVOS DE LAS ADMINISTRACIONES PÚBLICAS

Al margen de las normas vistas, la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, reconoce el derecho de los ciudadanos a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren. Por tanto, esta sería otra posibilidad para obtener los listados de acceso a las historias clínicas aunque teniendo que discutir numerosos matices que ahora no pretendemos abordar. Esto implicaría que para conocer quiénes han entrado en su historia, los ciudadanos también podrían recurrir a esta vía, si bien es cierto que teniendo que entrar en un procedimiento administrativo mucho menos contundente y expeditivo que la vía penal. Simplemente dejamos apuntada la posibilidad y el hecho de que todo el ordenamiento jurídico, de manera global, manifiesta una inequívoca tendencia a garantizar el derecho de los ciudadanos a obtener cuanta información tienen sobre ellos las administraciones.

7. DISCUSIÓN

Si algo parece que está meridianamente claro en nuestro ordenamiento jurídico es que el derecho a la libertad informática supone el derecho a controlar el uso de los datos incluidos en un programa informático y esto, en la práctica, implica que el interesado podrá exigir del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele, si hubiera lugar a ello. Por este motivo, las normas de protección de datos reconocen explícitamente el derecho de los ciudadanos a solicitar y obtener 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.

La Ley de autonomía del paciente y documentación clínica regula de forma taxativa quiénes y por qué motivos pueden acceder a una historia clínica, dejando así claro qué accesos no están autorizados. Los numerosos motivos que justifican la legitimidad

para entrar en una historia se pueden resumir en dos principios: El de vinculación asistencial y el de proporcionalidad, marcando entre ambos quién, cuándo y hasta dónde se puede acceder. No puede olvidarse que la propia ley establece que toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

Por otra parte, las leyes obligan a que queden identificadas, inequívoca y personalmente, todas las personas que acceden a una historia clínica. De cada 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. Esto es lo que de manera clara y didáctica se expresa diciendo que debe quedar registrado: "Quién, cuándo, desde dónde y a qué".

En algunas normas reguladoras de la historia clínica, como es el caso de la norma de la Comunidad Autónoma de Galicia, se establece la posibilidad de que dentro de la historia se creen, a petición del paciente, módulos de especial custodia para que los datos clínicos incluidos en ellos queden vedados incluso a otros profesionales que accedan a la historia, de modo similar a como la aplicación OMI contiene la posibilidad del uso del "Yo sólo". Las entradas en estos módulos quedarán singularizadas, creando así un doble registro de accesos. Esto se hace con el fin de permitir una mejor identificación de los accesos producidos y poder realizar auditorías específicas.

Llegados a este punto, podemos afirmar que para garantizar el derecho a la intimidad de los pacientes, el ordenamiento jurídico obliga a que exista un registro que ha de conservarse, al menos, durante dos años, en el que ha de constar, entre otros datos, la identificación de cuantas personas hayan accedido a la historia clínica. Incluso por parte de alguna comunidad autónoma se ha reforzado esta protección creando un doble sistema de registro, cuando pudiera producirse una trasgresión de datos especialmente dignos de protección. El propio Ministerio de Sanidad, al diseñar la Historia Clínica Digital para el Sistema Nacional de Salud, ha incluido la posibilidad de que el paciente pueda acceder digitalmente a este "registro de accesos".

Sin embargo, no todo está tan claro. Si empezamos a leer la letra pequeña empiezan a aparecer las sorpresas. El Ministerio de Sanidad proclama sin pudor que el ciudadano actúa como auditor externo del sistema para verificar y auditar el correcto cumplimiento de la ley en relación con los accesos que se hayan podido realizar por terceros a sus propios datos. Sin empacho ninguno afirma que el ciudadano puede realizar el seguimiento de los detalles de los accesos realizados desde este sistema a sus propios conjuntos de datos, a fin de poder verificar la legitimidad de los mismos, pero la sorpresa aparece cuando dice, a continuación, que "Dispondrá para ello de información relativa al momento en que se realizó el acceso, Servicio de Salud, centro sanitario y servicio desde el que se realizó cada acceso, así como las características del documento electrónico accedido". Vemos que el paciente tiene derecho a saber desde dónde se accedió y a qué, pero no quién accedió. El Ministerio de Sanidad desarrolla una herramienta de historia clínica digital para todo el país y de antemano considera pomposamente a los ciudadanos auditores externos del sistema, para, a reglón seguido, decir que no tienen derecho a saber quiénes concretamente han accedido legal o ilegalmente a sus datos de salud. ¿Si alguien detecta que se han producido accesos desde un servicio correspondiente a un centro sanitario de un Servicio de Salud en el que no ha estado en nunca, tiene algún derecho más? ¿Puede garantizar el Ministerio que el "paciente-auditor-externo" tiene alguna posibilidad de exigir la identidad de quienes, incumpliendo la Ley, han accedido a sus datos de salud? Tan sólo con leer el texto editado por el departamento ya se contestan las preguntas. En ningún momento habla de identificaciones personales de los intrusos en la intimidad.

De todos modos esto no es nuevo. Hace ya años que la Agencia Española de Protección de Datos viene interpretando que los pacientes no tienen derecho a saber quiénes han accedido a su historia clínica. Afirma, de manera rotunda y reiterada, que la revelación de los nombres de los facultativos o personal que atendió a un paciente no se encuentra amparada por el ejercicio del derecho de acceso. En un caso concreto, asimila, con pleno sentido común, a los profesionales que atendieron a un paciente con los que accedieron a su historia y sin embargo, a continuación, considera que el paciente no tiene derecho a conocer sus identidades. Esto es un sinsentido, máxime si tenemos en cuenta que la Ley de Ordenación de las profesiones sanitarias, establece que los profesionales y los responsables de los centros sanitarios facilitarán a sus pacientes el ejercicio del derecho a conocer el nombre, la titulación y la especialidad de los profesionales sanitarios que les atiendan. Es difícil poder decirlo más claro. Si el paciente tiene derecho a conocer el nombre de quien le trata y la AEPD

entiende que eso es sinónimo de conocer quiénes han accedido a su historia clínica, resulta inexplicable que se le niegue el referido derecho.

El problema es que las tesis restrictivas de la AEPD, de la Agencia de Protección de Datos de la Comunidad Autónoma de Madrid y del propio Ministerio de Sanidad están propagándose. Recientemente, la norma reguladora de la historia clínica de la Comunidad de Castilla La Mancha ha abierto el fuego de lo que pudiéramos calificar de normas autonómicas restrictivas del derecho de acceso a los "registros de acceso". Niega al paciente el derecho a recabar la identificación de las personas que, dentro del ámbito de organización del responsable del fichero, hayan podido tener acceso a la misma.

Lo que no deja claro la norma castellano manchega es si sólo excluye del derecho de acceso a los ciudadanos los datos identificativos de quienes han accedido legítimamente a la historia en el ejercicio de sus funciones "dentro del ámbito de organización del responsable del fichero" o si la exclusión es extensiva a todos aquellos que hayan accedido a la historia debida o indebidamente. ¿Significa esto que la administración sanitaria se está atribuyendo la competencia de determinar qué accesos se han efectuado en el ejercicio de funciones y cuáles no, de manera que informará al usuario de los accesos que ella considere que no se han ejercido dentro del ejercicio de las correspondientes funciones o por el contrario no piensa informar de ningún acceso cualquiera que sea su calificación? Sea de una manera u otra, lo cierto es que de manera expresa declara que los ciudadanos no tienen derecho a saber quiénes han accedido a sus historiales clínicos.

Del amplio derecho a saber "Quién, cuándo, desde dónde y a qué", que inicialmente parecía un inequívoco derecho declarado por el ordenamiento jurídico y su interpretación por los más altos tribunales del Estado, hemos pasado al "cuándo, desde dónde y a qué", haciendo desaparecer como por arte de magia el "Quién". Cómo si ello no fuera lo más relevante.

Decimos que el "quién" es lo más relevante porque el Código Penal establece que el acceso a la historia clínica por quien no esté legitimado para ello, es un delito. Delito que se consuma por el mero acceso sin necesidad de divulgar los datos a los que se haya accedido, lo que constituiría otro delito diferente. Además, se trata de un delito sólo perseguible mediante denuncia de la víctima, con la excepción de que el autor sea un funcionario público. Esto significa que los accesos indebidos a una historia clínica quedarán impunes si el paciente no tiene conocimiento de la identidad de los autores para poder denunciarlos. Tan sólo en el caso de que los autores del delito fuesen trabajadores públicos cabría la posibilidad de iniciar acciones contra ellos, pero ello dependería de que los responsables del fichero conociesen los hechos y los pusiesen en conocimiento de la autoridad judicial. Es decir, una vez más la defensa de los intereses del paciente quedaría en manos de la administración sanitaria.

7.- CONCLUSIONES

El problema que se plantea es determinar si el paciente tiene derecho o no a conocer quiénes han accedido a su historia clínica como una forma de garantizar su derecho a la protección de datos y a la intimidad.

Del conjunto de normas que regulan la protección de datos y la historia clínica se extrae de forma indubitada que el paciente tiene derecho a que, además de que se respete el carácter confidencial de los datos referentes a su salud, nadie pueda acceder a ellos sin previa autorización amparada por la ley.

Las leyes regulan de forma taxativa quiénes y por qué motivos se puede acceder a una historia clínica y obligan a que queden identificadas, inequívoca y personalmente, todas las personas que acceden, debiendo quedar esto anotado en un registro que ha de conservarse.

El Código Penal, y en consonancia con él, la jurisprudencia, considera constitutivo de delito el acceso a la historia clínica por quien no esté autorizado para ello y se trata de un delito, en principio, que para su persecución exige denuncia de la víctima.

La única forma que existe para garantizar que el paciente pueda ejercer las acciones pertinentes para proteger su derecho a que no se produzcan intromisiones ilegítimas en su intimidad, en forma de accesos indebidos a la historia clínica, es reconociendo su derecho de acceso al registro de los accesos producidos y que pueda solicitar cuanta información estime pertinente sobre la legitimidad de los mismos. No vemos inconveniente en entender que los accesos son equiparables a las cesiones, tal como hace en alguna ocasión la propia AEPD o bien considerando este derecho como una figura independiente y desligada del derecho de acceso a los ficheros informáticos, pero

proporcionando los listados de usuarios a fin de garantizar realmente la protección de la intimidad.

Si la actual regulación legal no bastase para reconocer el derecho de los pacientes a saber quiénes han tenido acceso a sus historiales médicos, los centros e instituciones sanitarias tiene el deber ético de hacer una interpretación de las normas que resulte favorable a esta pretensión. Los intereses en juego así lo exigen. No comprendemos cuáles son los bienes en confrontación. Frente al derecho a la intimidad del paciente se está oponiendo un inexistente derecho de los profesionales, que han accedido lícitamente para el desempeño de su actividad, a que no se lleve a cabo su identificación personal, contraviniendo así de forma expresa lo establecido en la ley. Sería impensable que lo que se pretende defender es la no identificación de quienes han accedido indebidamente, es decir, delictivamente.

Las interpretaciones restrictivas que propugnan la AEPD, el Ministerio de Sanidad y alguna norma autonómica, no son más que trabas con escaso sustento legal y que tan sólo conducirán a una mayor judicialización de las relaciones de los ciudadanos con el sistema sanitario. La situación de indefensión en la que queda el ciudadano es tal, que como decíamos al principio, solo cabe el recurso a la jurisdicción penal para tratar de dar solución a una inexplicable situación de hecho. Salvo que los ciudadanos estén dispuestos a dejar en manos de los centros sanitarios la decisión sobre la legalidad de los accesos a sus historias, si se les niega, cuando así lo soliciten, el conocimiento de quiénes han tenido acceso a las mismas, se verán obligados a interponer las correspondientes denuncias en busca del amparo judicial.