InDret
REVISTA PARA EL ANÁLISIS DEL DERECHO
WWW. INDRET.COM

Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias

Andrea Salud Casanova Asencio
Contratada predoctoral (FPU-MECD)
Departamento de Derecho Civil de la Universidad de Murcia

BARCELONA, ABRIL 2019

Abstract[*]

La historia clínica se caracteriza por contener una serie de datos de carácter personal –los datos de salud-, cuya conexión con la intimidad de la persona determina el establecimiento de un gran número de cautelas para su tratamiento por parte de la legislación vigente; especialmente, desde la implementación de los sistemas de historia clínica electrónica, susceptibles de permitir el acceso a dichos datos a un gran número de personas. Por ello, dicho acceso debe estar siempre justificado por una de las finalidades legalmente previstas, entre las que destaca la que tiene por objeto la prestación de la debida asistencia sanitaria. En este sentido, deben estudiarse cuáles son las condiciones precisas para que esta finalidad ampare el acceso a la historia clínica por parte del personal sanitario -toda vez que, en su defecto, el acceso se calificaría como ilegítimo-, así como las consecuencias del acceso no justificado por la finalidad asistencial. En el presente trabajo se analizan estos aspectos y se examinan las distintas cuestiones que presentan, exponiéndose además el estado de la cuestión tras la aprobación de la nueva normativa de protección de datos.

Medical history is a record which contains a series of personal data –concretely, health data- that, in consideration of their impact on people's intimacy, can only be managed under a good number of safeguards, according the current Spanish regulation; especially, since systems of electronic medical history have been implemented, as they permit a never-seen-before accessibility, thus making said data available to a greater number of people. Hence, the access must always be justified by one of the legally provided purposes, as is the one associated with the supplying of the adequate health care. In this sense, the specific conditions that must be met in order to justify the access of sanitary personnel to the medical history, much as the consequences of the unjustified access, must be examined. In the present work this analysis is addressed, taking into account the provisions of the implementation of the new data protection laws.

Title: Data protection and medical history: the unjustified access by health personnel and its consequences

Keywords: personal data, health data, medical history, medical record, data access, data traceability, right to access, health personnel, health care, unjustified access, consequences, confidentiality, new regulation, data protection, General Data Protection Regulation, GDPR.

Palabras clave: datos personales, datos de salud, historia clínica, acceso, trazabilidad de los datos, registro de accesos, derecho de acceso, personal sanitario, vinculación asistencial, finalidad asistencial, acceso ilegítimo, acceso injustificado, consecuencias, confidencialidad, nueva legislación, protección de datos, LOPD, nueva LOPD, Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales, LOPDGDD, Reglamento General de Protección de Datos, RGPD.

[*] Financiación otorgada por el Ministerio de Educación, Cultura y Deporte de acuerdo con la Resolución de 19 de noviembre de 2015, por la que se convocan Ayudas para la Formación de Profesorado Universitario.

Sumario

1. Historia clínica electrónica y datos de salud

La historia clínica, que el artículo 14.1 de 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 (BOE nº 274, de 15.11.2002) (en adelante, LAP) describe[1] como el instrumento que "comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro", es un mecanismo imprescindible para los profesionales que posibilita el acceso tanto a los antecedentes clínicos del paciente como a diagnósticos y tratamientos emitidos por parte de otros profesionales, del mismo o distinto centro, y de la misma o distinta especialidad médica[2], que al mismo tiempo redunda en claro beneficio de los pacientes[3].

[1] Además, el artículo 3 recoge una serie de definiciones, entre las que se encuentra la de historia clínica: "el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial".

[2] Suponiendo así, también, como asimismo indica MILLÁN CALENTI, un medio de comunicación entre los distintos profesionales médicos (2013, p. 784).

[3] MILLÁN CALENTI remarca este aspecto al decir que "la histórica clínica electrónica se basa en la aplicación de las tecnologías de la información al ámbito de la actividad sanitaria, con el objetivo de facilitar el acceso a la misma en

Superado el viejo sistema de documentación de la historia clínica en formato papel, la historia clínica electrónica permite que toda la información relativa al historial clínico del paciente se encuentre centralizada y sea accesible[4] por parte de los profesionales sanitarios. Sin embargo, esa accesibilidad no deja de entrañar grandes riesgos para el paciente cuyos datos se consignan en el mismo, tanto más cuanto más sensibles son los datos a consignar y mayor es el número de personas que tiene acceso a ellos[5].

Ésta es una circunstancia que ha de valorarse, especialmente, en el contexto de una sociedad en la que el desarrollo de la tecnología permite el acceso y traspaso de cualquier tipo de datos de una forma casi inimaginable tiempo atrás, máxime en el caso de la historia clínica, teniendo en cuenta que hablamos de datos cuyo tratamiento es ciertamente delicado, y que a la misma pueden acceder –al menos, potencialmente- miles de profesionales (por no hablar de los ulteriores trasvases de información a terceros que pueden producirse).

Y es que no debe olvidarse que los datos personales y, en particular, los datos de salud, están estrechamente vinculados con la intimidad de la persona[6], como se desprende, además, del artículo 7 LAP, y que, bien por su propio contenido[7], bien por la posible finalidad de su uso potencial, son datos particularmente vulnerables, merecedores de una protección específica por parte del Ordenamiento jurídico, que se encarga de establecer, a través de la legislación de protección de

cualquier momento y lugar que el paciente lo necesite, independientemente de donde se haya generado esa información" (2013, p. 780).

[4] PEREIRA ÁLVAREZ habla de un "escenario de integración y accesibilidad" traído por la historia clínica electrónica (2009, p. 309).

[5] Ésta es la consigna de la que parte el documento *Ética en el acceso y en el uso de la documentación clínica: reflexiones y recomendaciones,* preparado por el Consello de Bioética de Galicia y publicado en 2017, tras la práctica ofrecida por la puesta en vigor del Decreto 29/2009, de 5 de febrero, por el que se regula el uso y el acceso a la historia clínica electrónica en Galicia, norma pionera en esta materia. Por otra parte, así se han pronunciado también autores como ORDÁS ALONSO (2016, pp. 774, 775). Sin embargo, desde otro punto de vista la historia clínica electrónica ha sido vista como una herramienta que asegura una mayor protección de los datos que la historia clínica en papel, por imponer la necesidad de identificación para el acceso y la trazabilidad de los mismos (ETREROS HUERTA, 2009, p. 186). En el mismo sentido, SÁNCHEZ CARO, 2009, p. 58, y TRONCOSO REIGADA, para quien, a pesar de que las tecnologías pueden provocar mayores vulneraciones a los derechos que un acceso indebido en papel (por escandalosos que puedan ser algunos ejemplos, como el de las historias clínicas abandonadas en la calle), la mejor manera de velar por la seguridad de los datos clínicos es su traslado a soportes informáticos (TRONCOSO REIGADA, 2006, pp. 84, 85, 137, 142).

[6] Un derecho, recordemos, reconocido constitucionalmente (art. 18.1 CE), y relacionado con la dignidad de la persona (SERRANO PÉREZ, 2013, p. 1095). Sin perjuicio de la conexión entre el derecho a la intimidad y el derecho a la protección de los datos personales, se ha considerado que éste último, que además se entiende incluido artículo 18.4 CE –el propio artículo 1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como su Preámbulo, lo dicen claramente-, es autónomo con respecto al primero (GONZÁLEZ GARCÍA, 2014, p. 274). En el mismo sentido y con mayor profundidad sobre el derecho a la protección de datos como derecho autónomo, ORDÁS ALONSO, 2016, pp. 780, 781 y 788 a 792. También se refleja esta concepción en la jurisprudencia del Tribunal Constitucional (STC, 20.7.1993 [RTC 1993/254; MP: Fernando García-Mon y González Regueral]) y del Tribunal Supremo (véase la STS, Sala 2ª, 4.7.2016 [RJ 2016/2856, MP: Manuel Marchena López] y las que la citan).

[7] En el tratamiento de los datos de salud, contrariamente a como ocurre con los datos ordinarios, el riesgo puede provenir directamente del contenido del dato, independientemente de la finalidad de dicho tratamiento (BARRAL, 2011, p. 353).

datos, especialidades -cuando no limitaciones o prohibiciones- en cuanto a su tratamiento.Así lo hace el artículo 9 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE nº 119, de 4.5.2016) (en adelante, RGPD, o, simplemente, Reglamento), que en su apartado primero prohíbe el tratamiento de los datos de salud (entre otras "categorías especiales de datos personales", según la rúbrica del artículo), los cuales, no obstante, podrán ser objeto de tratamiento en algunos casos indicados por la norma, entre los que se incluye la prestación de asistencia sanitaria (apartados 3 y 2.h). Ha de decirse que el RGPD es una norma de aplicabilidad directa en nuestro Ordenamiento a partir de su entrada en vigor el 25 de mayo de 2018, y que ofrece una regulación que se ha considerado más detallada y garantista[8] que la dispuesta por la que hasta hace poco era la normativa española de referencia en la materia, esto es, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE nº 298, de 14.12.1999) (en adelante, LOPD), derogada recientemente en virtud de la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE nº 294, de 6.12.2018) (en adelante, LOPDGDD), que adapta el Ordenamiento español al modelo establecido por el Reglamento y completa el marco normativo en la materia; marco normativo que, en consecuencia, resultará de aplicación en caso de que se produzca un acceso a los datos que pueda ser considerado como ilegítimo o injustificado.

No obstante, para hablar de acceso ilegítimo es imprescindible conocer previamente cuándo un acceso tiene o no, precisamente, este carácter. A este respecto, hay que acudir al artículo 16 de la LAP, que relaciona una serie de finalidades que ampararían el acceso a la historia clínica y determinarían la clasificación del acceso como legítimo o justificado. Esta previsión legal engarza, a su vez, con el artículo 7.1 LAP, que dispone que nadie podrá acceder a los datos referentes a la salud de las personas sin que medie la debida autorización amparada por la Ley al respecto; autorización legal que sin duda se encuentra en dicho artículo 16 de la misma Ley.

Pues bien, entre las finalidades recogidas por el artículo 16 LAP se encuentran la finalidad asistencial (art. 16.1); el acceso con fines de investigación, docencia, epidemiología, de salud pública, o judiciales (art. 16.3); o el acceso con fines de inspección, evaluación, acreditación y planificación (art. 16.5). Aún más, en ésta y otras normas se regulan casos excepcionales en los que terceros ajenos al ámbito sanitario pueden tener acceso a estos datos[9], o cuestiones tales como el derecho del propio interesado a acceder a su historia clínica[10].

[8] Entre otras razones, por incluir, en su artículo 4.15, un concepto más amplio de lo que sean los datos de salud, recogiendo así el testigo de diversos estudios y trabajos publicados bajo la vigencia de la antigua Directiva, como es la conceptualización que realizaba el Grupo de Trabajo del Artículo 29 en el año 2015 (ÁLVAREZ RIGAUDIAS, 2016, pp. 173, 174).

[9] Algunos de los supuestos del art. 9.2 RGPD; art. 18.4 LAP.

[10] Art. 15 del Reglamento; art. 13 LOPDGDD; art. 18 LAP.

De entre todas estas cuestiones, se va a tratar únicamente la relativa al acceso a la historia clínica con fines asistenciales, con el fin de conocer cuándo está legitimado el personal sanitario para acceder a estos datos según dicho parámetro, y cuándo, de no estarlo, nos encontraremos ante un acceso ilegítimo, para posteriormente analizar sus posibles consecuencias y la influencia que la nueva legislación en materia de protección de datos tiene en esta materia.

2. El acceso a la historia clínica justificado por la finalidad asistencial

2.1. Finalidad asistencial y acceso legítimo. Los principios de vinculación asistencial y de proporcionalidad

El artículo 16.1 LAP indica que la historia clínica es "un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente", añadiendo, además, que "los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia". Puede decirse que la finalidad asistencial es, con seguridad, la principal y primera causa justificativa del acceso a la historia clínica.

Así, la historia clínica aparece como elemento necesario e inherente al tratamiento médico[11], y el acceso a la misma se configura como un deber del personal sanitario, que está obligado a acceder a dichos datos para prestar su servicio adecuadamente[12]. Este deber queda garantizado por el artículo 16.2 LAP[13], al indicar que cada centro establecerá los mecanismos oportunos para posibilitar en todo momento el acceso a la historia clínica de cada paciente por el personal que le asista, e implica la concesión de unas facultades de acceso que en ocasiones han motivado que se hable de las mismas como si de un *derecho* del personal sanitario se tratara[14]; algo que, desde el rigor técnico, no parece que pueda afirmarse[15].

[11] Así lo indica el Informe *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGDP* presentado por la Sociedad Española de Salud Pública y Administración Sanitaria en 2017 (en adelante, Informe SESPAS), p. 52. También la tilda de "instrumento necesario" TRONCOSO REIGADA, subrayando su vinculación con los derechos constitucionalmente reconocidos a la vida (artículo 15 CE) y a la protección de la salud (artículo 43 CE) (2006, pp. 45, 46). Para GÓMEZ PIQUERAS, la historia clínica es "el instrumento básico del buen ejercicio sanitario" (2009, p. 134).

[12] Dice TRONCOSO REIGADA que "no hay opción, hay un deber de todo profesional sanitario de hacer historia clínica" (2006, p. 70). Incide en esta idea el primer punto del Decálogo de la Historia Clínica aprobado en febrero de 2017 por la Comisión Central de Deontología de la Organización Médica Colegial de España y la Comisión Permanente del Consejo General de Colegios Oficiales de Médicos, que indica que se trata de un derecho del paciente y un deber del médico.

[13] Y se corresponde, a su vez, con el de paciente de facilitar sus datos sanitarios de manera veraz (art. 2.5 LAP).

[14] La doctrina insiste en la doble vertiente de la historia clínica como derecho y deber del médico, como puede verse, entre otros, en SÁNCHEZ CARO, 2009, p. 68, o en BARRAL, 2011, p. 364.

[15] Es muy importante advertir aquí que, desde el punto de vista jurídico-técnico, no parece posible hablar de un verdadero derecho del personal sanitario al acceso a la historia clínica de sus pacientes: ciertamente, no se trata de un derecho subjetivo que pueda ser protegido por el Ordenamiento ni ejercitado en sede judicial, por nombrar sólo alguna de las consecuencias que conocidamente se derivan de los mismos. Por tanto, será recomendable no emplear dicho término para referirse a lo que más bien es una herramienta del médico para el correcto cumplimiento de los

Esta necesaria concurrencia de una finalidad asistencial como justificativa del acceso a los datos de salud del paciente de la que venimos hablando es lo que se conoce como *principio de vinculación asistencial*. Éste es un principio básico en esta materia que aparece, como señalan varios autores[16], acompañado por el *principio de proporcionalidad*, que determina que el profesional deba acceder únicamente a los datos mínimos necesarios para prestar la asistencia sanitaria concreta.

Estos dos principios, conjuntamente considerados, delimitarán en cada caso la concurrencia de esa finalidad asistencial respecto del acceso a los datos concretos, y, en consecuencia, los contornos del acceso legítimo a los mismos[17]; a sensu contrario, todas aquellas incursiones que sobrepasen los límites por ellos marcados habrán de ser consideradas injustificadas –a menos que se encuentren amparadas, claro está, por alguna de las otras finalidades previstas en el artículo 16 LAP-, y podrán determinar el advenimiento de una o más de las consecuencias previstas para este tipo de supuestos.

2.2. El deber de confidencialidad

Además de los principios de vinculación asistencial y de proporcionalidad, existe un deber que debe regir toda relación asistencial, así como cualquier actuación que implique entrar en contacto con los datos de salud del paciente: hablamos del deber de confidencialidad.

En esta materia, se ha de partir del deber de confidencialidad que de modo general dirige el artículo 5 LOPDGDD a los responsables y encargados del tratamiento de datos y a todos los que intervengan en cualquier fase del mismo (artículo 5.1), especificando, además, que está obligación general será complementaria a los deberes de secreto profesional que deban observarse según la normativa aplicable en cada caso (artículo 5.2). Por otra parte, el RGPD hace una llamada general al deber de confidencialidad en el tratamiento de los datos personales en su artículo 5.1.f), lo cual es señal inequívoca de su importancia.

De manera más concreta, el deber de confidencialidad adquiere una enorme relevancia en el ámbito sanitario[18], por las características de los datos a tratar y porque, al fin y al cabo, este deber se presenta como uno de los pilares de la especial relación de confianza médico-paciente[19], y es por

deberes inherentes a su trabajo, y tener en cuenta, cuando nos topemos con su lectura en cualquier texto, que probablemente se mencionará con un sentido más bien laxo y no estrictamente técnico.

[16] SÁNCHEZ CARO, 2009, p. 68; PEREIRA ÁLVAREZ, 2009, p. 311; GONZÁLEZ GARCÍA, 2014, p. 277; Informe SESPAS, p. 53.

[17] GALLEGO RIESTRA y RIAÑO GALÁN lo expresan así: "Los numerosos motivos que justifican la legitimidad para entrar en una historia clínica 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" (2012, pp. 86, 87).

[18] Sobre el derecho a la intimidad y el secreto médico como expresión concreta de dicho derecho en el ámbito sanitario es de interés la obra de DE MIGUEL SÁNCHEZ (2002).

[19] Y, en general, de la relación entre el paciente y el personal sanitario que le atiende, toda vez que el primero se vincula, más que a un facultativo concreto, al servicio sanitario público al que el paciente se encuentra asignado, sin que ello provoque un menoscabo para los derechos del paciente, como indica el Tribunal Constitucional en su

ello que son varias las normas que amparan el deber de confidencialidad como principio rector de la relación asistencial.

Así, se han de remarcar, en primer lugar, la mención expresa realizada en el artículo 9.3 del RGPD[20], así como la del artículo 10.3 de la Ley 14/1986, de 25 de abril, General de Sanidad (BOE nº 102, de 29.4.1986)[21]. En el mismo sentido se pronuncian el artículo 7.1 de la LAP, en términos que resultan muy claros[22], y el artículo 16.6 de la misma Ley.

Otro punto destacable de la regulación del deber de confidencialidad es que éste se extiende a toda persona que tenga acceso a los mismos, y no únicamente a aquéllas cuya profesión esté específicamente sujeta al deber de secreto profesional[23], como se encarga de subrayar el artículo 2.7 LAP, que es casi una cláusula de cierre del sistema. Esto último va, además, en consonancia con lo previsto por la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen (BOE nº 115, de 14.5.1982) en su artículo 7.4, que indica que tendrá carácter de intromisión ilegítima la revelación[24] de los datos conocidos a través de la actividad profesional de quien los revela, sin circunscribirse a aquellas profesiones sujetas específicamente a un deber de secreto profesional (ni tampoco, lógicamente, al ámbito sanitario). Esta misma norma prevé también que, para la tutela de los derechos a los que la misma se refiere, podrá el perjudicado acudir, además de a las vías procesales ordinarias, al procedimiento previsto por el artículo 53.2 de la Constitución y, cuando proceda, al recurso de amparo frente al Tribunal Constitucional.

Al margen de estas normas, se ha de destacar que el deber de confidencialidad es asimismo considerado un deber de tipo deontológico, por lo que muchos otros textos de este ámbito inciden también en la cuestión[25].

Auto de 11.12.1989 (RTC 1989/600; MP: desconocido; Magistrados: Miguel Rodríguez-Piñero y Bravo-Ferrer, Antonio Truyol Serra y Álvaro Rodríguez Bereijo).

[20] Este artículo realiza una mención expresa del secreto profesional en el ámbito de la asistencia sanitaria que ha sido recibida positivamente por la doctrina, como puede verse en el Informe SESPAS (p. 50).

[21] Artículo que indica, como derecho de "todos" frente a las administraciones públicas sanitarias, el relativo a "la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas", extendiendo además esta previsión a aquellas entidades sanitarias privadas que presten colaboración al sistema público.

[22] Su regulación del principio de confidencialidad ha sido destacada como una de sus mayores innovaciones (PALACIOS PALACIOS y ESCUDERO GONZÁLEZ, 2011, p. 266).

[23] Lo cual implicaría una extensión del deber de confidencialidad (BARRAL, 2011, p. 364).

[24] La LO 1/1982 sólo comprende en su ámbito de aplicación la conducta compuesta por la revelación de los datos, y no el mero acceso a los mismos; cuestión en la que ahondaremos más adelante.

[25] Así lo hacen la práctica totalidad de los Códigos Deontológicos, que establecen importantes consecuencias ante el quebrantamiento del deber de secreto profesional en el ámbito de los Colegios Profesionales, como se verá, u otros documentos como el Decálogo de la Historia Clínica (2017) antes citado.

3. Consecuencias del acceso indebido a la historia clínica

Es evidente que, dado el carácter particularmente vulnerable de los datos de salud, el objetivo principal del Ordenamiento en cuanto a su protección debe ser el establecimiento de medidas que impidan que se efectúe cualquier tipo de acceso injustificado a dichos datos, y en este sentido se manifiesta la nueva normativa de protección de datos, que busca que el responsable de los mismos adquiera una responsabilidad que en el Reglamento se ha denominado como "proactiva" (véase el artículo 5.2 RGPD), de manera que, una vez evaluado el riesgo que para los datos personales puede suponer el tratamiento a realizar, establezca las salvaguardas adecuadas desde el propio diseño del sistema (art. 25 RGPD). Existen, así, un buen número de mecanismos cuya finalidad es, precisamente, la de evitar que dicho acceso ilegítimo llegue siquiera a darse[26].

Sin embargo, la práctica demuestra que es imposible, o, al menos, muy difícil excluir por completo la posibilidad de que dichos accesos ilegítimos se efectúen[27]. Y ello en atención a razones de diversa índole: por una parte, las propias exigencias del sistema, que debe garantizar la protección de la salud como valor principal. En este sentido, ha sido advertido, y con acierto, que la aplicación general de un sistema cerrado y poco flexible, además de ser compleja, puede poner en riesgo la salud del paciente; y es que es tan variada la casuística en la práctica que el establecimiento de criterios generales de acceso férreos puede ser contraproducente[28].

Por otra parte, no puede decirse que sea infrecuente en el marco de los hospitales y centros de salud encontrar un ordenador en el que un usuario anterior ha dejado su sesión *abierta*, de manera que, durante un lapso de tiempo más o menos prolongado hasta que la sesión se bloquea, en su caso, automáticamente, cualquier otro usuario tiene la oportunidad de acceder a las historias clínicas a las que el usuario anterior tuviera acceso[29]. Así como, en todo caso, y por muchas precauciones

[26] Puede verse, al respecto, CASANOVA ASENCIO, 2018.

[27] Una buena prueba de ello son las advertencias que realiza el Consello de Bioética de Galicia, en su documento *Ética en el acceso y en el uso de la documentación clínica* de 2017, antes citado, en el que reseñan una serie de datos demoledores en torno a la importancia práctica de este problema e inciden en la obligatoriedad para los profesionales sanitarios de observar el deber de confidencialidad, así como, entre otros, el deber de custodiar de manera correcta las claves de acceso individuales a la historia clínica, desvelando que, aún después de la puesta en marcha del sistema IANUS en el año 2009, sistema que cuenta con un buen número de mecanismos de prevención del acceso ilegítimo, en la práctica siguen aconteciendo múltiples casos de accesos de este tipo.

[28] SÁNCHEZ CARO, 2009, pp. 71, 72.

[29] Ésta es una de las razones, precisamente, por las que en la SAP Madrid, Sección 16ª, 13.3.2018 (ARP 2018/632; MP: Francisco David Cubero Flores) se absuelve a dos enfermeras acusadas de acceder ilegítimamente a la historia clínica de la denunciante. El Tribunal relata cómo de la abundante prueba testifical se desprende que es una práctica habitual en el centro de salud donde suceden los hechos "dejar los ordenadores abiertos cuando se consulta una historia clínica, de modo que otra persona puede venir después y aprovechando que la historia está abierta, consultarla", indicando que "la mera huella informática o digital que refleja una consulta de un profesional en una historia clínica acredita que se ha entrado con las claves de dicho profesional, pero no que dicho profesional sea precisamente quien accede", con la relevancia que este extremo tiene en cuanto a la destrucción de la presunción de inocencia en el ámbito penal. Ha de añadirse, además, que frente a esta sentencia se presentó recurso de casación, que fue inadmitido, reproduciéndose parte de los argumentos empleados en la sentencia de la Audiencia, en virtud de auto del Tribunal Supremo, Sala 2ª, 13.9.2018 (JUR 2018/300037; MP: Manuel Marchena Gómez).

Por otra parte, también trata esta cuestión, aunque resuelve de modo opuesto a resultas de la valoración del conjunto de medios de prueba aportados, la reciente STS, Sala 2ª, 23.10.2018 (RJ 2018/4717; MP: Luciano Varela

que se tomen, tampoco puede excluirse que una persona no autorizada a entrar en contacto con determinados datos pueda tratar de acceder a ellos por motivaciones diversas[30] (lo cual será más o menos arduo en función de la rigidez del sistema, que ya hemos dicho que en ningún caso podrá ser absoluta).

Finalmente, la realidad se impone y determina que, siendo imposible asegurar por completo que a la historia clínica sólo accederá quien efectivamente deba hacerlo, es imprescindible dotar al perjudicado, al propio Ordenamiento y a la sociedad en su conjunto[31] de una serie de vías de reacción frente al acceso ilegítimo y, así, frente al profesional que accede a los datos clínicos de una persona sin estar amparado por la vinculación asistencial que habría de justificar dicho acceso.
A continuación, se desgrana una relación de las consecuencias que este tipo de accesos ilegítimos pueden tener; consecuencias que tal vez, por su efecto disuasorio, pudieran también funcionar como posibles remedios frente a dichos accesos injustificados, y entre las que se cuentan algunas de Derecho Público y otras de Derecho Privado. En este análisis se abordarán los aspectos problemáticos que de varias de ellas se desprenden, teniéndose en cuenta las soluciones en cada caso aportadas por la nueva legislación de protección de datos.

3.1. Sanciones administrativas

El incumplimiento de la normativa de protección de datos puede acarrear la imposición de cuantiosas sanciones. De hecho, el Considerando 148 RGPD indica que, a fin de reforzar la aplicación de las normas presentes en el mismo, cualquier infracción deberá ser castigada con sanciones, "incluidas multas administrativas". A esta idea responde el artículo 83 del mismo cuerpo legal, que recoge las condiciones generales para la imposición de multas administrativas por parte de la autoridad de control estatal (que, en nuestro caso, es la Agencia Española de Protección de Datos), la cual tiene, además, otras potestades correctivas sobre las entidades o personas infractoras en virtud de lo dispuesto por el artículo 58.2 RGPD. Estas potestades habrán de estar sujetas en todo caso a garantías procesales adecuadas, entre ellas la tutela judicial efectiva, como indican tanto el apartado octavo del artículo 58 como el Considerando 148 del Reglamento.

Castro), que entiende que, en el caso que se enjuicia, la posibilidad de que otra persona hubiera accedido a los datos valiéndose de las claves de las personas acusadas es una "mera posibilidad teórica" no acreditada a la vista de la prueba practicada.

[30] Existen, precisamente, sentencias condenatorias por accesos indebidos al propio sistema IANUS de la Comunidad Autónoma gallega, como la SAP A Coruña, Sección 6ª, 8.10.2018 (JUR 2018/314374; MP: César González Castro) (a la que, por cierto, sigue una petición de indulto por parte del Tribunal sentenciador por entender que las penas que en virtud de norma han de imponer son demasiado severas), que demuestra que ningún mecanismo de prevención de los hasta ahora implementados llega a ser infalible, probablemente por los propios requerimientos del sistema (que, como decimos, ha de ser seguro pero flexible).

[31] No puede perderse de vista que es imprescindible mantener la confianza de la sociedad en el sistema sanitario desde el punto de vista de la salud pública. En este sentido, ORDÁS ALONSO incide en que el secreto médico no se encuentra establecido únicamente en interés del paciente, sino que existe un interés público en preservar la confianza de los ciudadanos en el sistema sanitario (2016, pp. 784, 785 y 792, 793). Del mismo modo, el Tribunal Europeo de Derechos Humanos ha subrayado en diversas ocasiones la importancia del mantenimiento del carácter confidencial de los datos de salud como mecanismo para preservar la confianza de los ciudadanos en los servicios de salud; y es que no hay más que imaginar el efecto que tendría una enfermedad infecciosa sobre una población en la que dicha confianza se encontrara quebrada (véase DE LA SERNA BILBAO y FONSECA FERRANDIS, 2017, p. 2285).

Prevé igualmente el artículo que los Estados miembros podrán establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos (apartado séptimo), además de disponer en su artículo 84 la posibilidad de que los Estados miembros puedan establecer otras sanciones aplicables distintas de las multas administrativas que, en palabras del artículo, sean "efectivas, proporcionadas y disuasorias".

Por lo que hace a la normativa española, el régimen de infracciones y sanciones por incumplimiento de la normativa de protección de datos se contiene en los artículos 70 y siguientes de la LOPDGDD, que relaciona un buen número de conductas activas y omisivas constitutivas de infracciones. Por lo que resulta aplicable al tema objeto de este trabajo, destaca como infracción muy grave la vulneración del deber de confidencialidad establecido en el artículo 5 de la Ley (art. 72.1.i)), además de la determinación como infracciones de otras circunstancias relacionadas con la falta de aplicación de las medidas técnicas y organizativas de seguridad que correspondan al tratamiento (véanse, por ejemplo, las letras d), e) y f) del artículo 73, dedicado a las infracciones de carácter grave), entre otras muchas que, a resultas de las propias exigencias del nuevo sistema, pudieran ser de aplicación, según el caso.

Para el caso de infracciones cometidas por entidades privadas, el artículo 76.3 prevé que, además de las sanciones que correspondan, de manera complementaria o alternativa a éstas, podrán imponerse las restantes medidas correctivas a las que se refiere el artículo 84.2 RGPD.

Por otra parte, y en relación a las entidades que recoge el artículo 77.1 (de carácter público o asimilado), se prevé que la autoridad competente dicte una resolución conteniendo un apercibimiento[32], así como las medidas de cesación de la conducta o correctoras que procedan (art. 77.2), disponiéndose además la posibilidad de proponer la iniciación de actuaciones disciplinarias, si procedieran, las cuales se regirían según lo dispuesto en la legislación sobre régimen disciplinario o sancionador que resultara de aplicación (art. 77.3).

3.2. Defensa de los derechos del perjudicado ante los Tribunales

La posibilidad de acudir a los Tribunales supone, sin duda, una de las herramientas más importantes a manos de los perjudicados por un posible acceso ilegítimo a los datos contenidos en la historia clínica. Sin embargo, y, como puede imaginarse, la posibilidad de que el propio interesado pueda instar un procedimiento judicial dependerá de que éste llegue a tener conocimiento de que dicho acceso ilegítimo se ha producido.

[32] Para TRONCOSO REIGADA no tiene sentido imponer una sanción económica a una entidad pública porque ello, a diferencia de lo que sucede con las entidades privadas, implica únicamente una redistribución de créditos o una modificación presupuestaria (2006, p. 65). Cabe añadir, además, que ello no dejaría de implicar el pago de una cuantiosa sanción con dinero procedente de las arcas públicas. A salvo queda, no obstante, el derecho del particular de pedir la responsabilidad patrimonial por el daño sufrido, que sí se concreta en una condena pecuniaria a la propia Administración. Precisamente por el apunte recién realizado en torno al origen del dinero es importante que se cumpla con la previsión del artículo 36 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (BOE nº 236, de 2.10.2015), relativa a la posibilidad de reclamar lo pagado por parte de la Administración al verdadero responsable de los hechos.

No son pocas las ocasiones en que el hecho llega a oídos del perjudicado, precisamente, porque la información llega a ser conocida por terceros que luego difunden los datos. No obstante, en otros casos en los que no se produce una comunicación a terceros de los datos, sino sólo un mero acceso a los mismos por parte del profesional no autorizado, es preciso que se establezcan una serie de mecanismos para que el perjudicado pueda tomar conocimiento de estos accesos. En este sentido, pueden apuntarse opciones como el registro de accesos o la figura de la quiebra de seguridad, de las que más adelante hablaremos.

Así las cosas, una vez que el afectado, por el medio que sea, tiene conocimiento o alberga sospecha del acceso ilegítimo a sus datos, tiene varias vías de actuación a su disposición para procurar la defensa de sus derechos en sede jurisdiccional.

De manera general, el artículo 77.1 del Reglamento recoge la posibilidad de presentar reclamación ante la autoridad de control, y ello "sin perjuicio de cualquier otro recurso administrativo o acción judicial", según la literalidad del artículo, para pasar a reconocer expresamente el derecho a la tutela judicial efectiva de los afectados frente a dicha autoridad de control y frente al responsable o encargado del tratamiento de los datos en los artículos 78 y 79, respectivamente.

Además, respecto de las conductas que pudieran revestir caracteres de delito, indica el Reglamento en su considerando 149 que los Estados podrán tipificar como delito conductas que supongan infracciones en el sistema del Reglamento, siempre que se respete el principio *ne bis in idem*.
En nuestro Ordenamiento, el acceso indebido es susceptible de dar lugar a ilícitos de diverso orden, pudiendo, así, encauzarse la tutela judicial de los derechos del afectado a través de varias jurisdicciones.

a. Condenas por la responsabilidad civil dimanante del daño causado a propósito del acceso ilegítimo a la historia clínica

El artículo 82.1 RGPD[33] recoge expresamente el derecho a la indemnización de los daños causados a sus particulares, debiendo asegurarse, según puede leerse en el Considerando 146, que los interesados "reciban una indemnización total y efectiva por los daños y perjuicios sufridos".
Existen numerosos ejemplos en la práctica en los que se condena por los daños causados como consecuencia del acceso indebido a la historia clínica, tanto en sede contencioso-administrativa (para los centros sanitarios públicos), como en sede civil (al dilucidar la responsabilidad de los centros sanitarios privados, pero también la del personal sanitario de centros públicos individualmente considerado o, en general, al ejercitar la acción directa contra las aseguradoras de centros públicos o privados).

[33] El artículo 19 de la derogada LOPD se refería expresamente al derecho a indemnización de los particulares por los daños que hubieren sufrido; mención que la actual LOPDGDD suprime, probablemente con acierto, ya que se trataría de una previsión un tanto superflua y reiterativa a la vista de que el RGPD ya se refiere a la cuestión y de que, además, los principios generales que en nuestro Ordenamiento rigen la responsabilidad de la Administración Pública, por un lado, y la de los particulares, por otro, siguen rigiendo en esta materia (regímenes a los que, además, el propio artículo 19 LOPD se remitía).

En el ámbito contencioso-administrativo pueden verse ejemplos tan destacados como el de la STSJ Navarra, Sala de lo Contencioso-Administrativo, Sección 1ª, 8.2.2012 (RJCA 2012/143; MP: Antonio Rubio Pérez), en la que se condena al Servicio Navarro de Salud por el mal funcionamiento del servicio público[34] al haberse registrado la cantidad de 2.825 accesos a la historia clínica de una paciente que sólo estuvo en un hospital y en cuatro servicios, por parte de 417 usuarios integrados en 55 servicios, que accedieron, al parecer, por lo llamativo de sus lesiones[35]. Es posible, por tanto, condenar al servicio de salud público por los daños causados al particular, sin perjuicio de que en sede contencioso-administrativa puedan dilucidarse otras cuestiones ajenas a la reparación del daño pero que también aparecerían como consecuencia del acceso injustificado a la historia clínica (así, por ejemplo, la imposición de multas administrativas, o la imposición de sanciones disciplinarias al personal de la Administración, según se ha visto ya). Hay que recordar, por otra parte, que el artículo 36 de la Ley 40/2015 de Régimen Jurídico del Sector Público dispone el derecho de la Administración condenada a exigir a las autoridades y personal público a su servicio la responsabilidad patrimonial que proceda por los daños por éstos causados mediando dolo, culpa o negligencia graves, así como un procedimiento administrativo para hacer efectivo este derecho.

En el ámbito civil, por otro lado, donde la cuestión adquiere relevancia únicamente a efectos de resarcir el daño causado, han recaído sentencias como la STS, Sala 1ª, 27.1.1997 (Roj 452/1997; MP: José Almagro Nosete), que confirma la condena al establecimiento sanitario por responsabilidad civil extracontractual, con base en los artículos 1902 y 1903 CC, por haberse producido filtraciones de la historia clínica de un paciente con SIDA, según consta en la sentencia, a consecuencia de haber dejado desatendida la documentación clínica de un paciente, la cual terminó en manos de terceros que usaron dicha información para chantajear al afectado.

Aún más, se ha de recordar que, como se ha dicho antes, es posible acudir a la tutela constitucional en amparo por violación de los derechos fundamentales a la intimidad, honor y propia imagen, consagrados por la LO 1/1982, siendo un buen ejemplo de ello la STC, 14.2.1992 (RTC 1992/20; MP: Francisco Tomás y Valiente), en la que se condenaba, de nuevo, por la difusión (en este caso, periodística) de la circunstancia del paciente de ser enfermo de SIDA.

b. Condena penal por el acceso indebido a la historia clínica

Además del resarcimiento del daño causado por el acceso injustificado a la historia clínica en cualquiera de los órdenes jurisdiccionales vistos, el Código Penal prevé, en los artículos 197 y siguientes, una serie de tipos específicos para los delitos de descubrimiento y revelación de secretos

[34] Dice la sentencia, textualmente, que "la organización sanitaria tiene, probablemente, una dificultad a la hora de conciliar el derecho de los pacientes a su intimidad y propia imagen con el libre acceso de los profesionales a la historia clínica", determinando que este tipo de acceso no puede ampararse en razones asistenciales.

[35] Según puede leerse en la resolución, la historia clínica contenía fotografías de las lesiones, en alguna de las cuales se incluía el rostro de la paciente, de manera que era posible determinar su identidad. El fallo incluye, también, la obligación de retirar dichas fotografías de la historia clínica.

que resultan aplicables a esta clase de supuestos[36], tanto si se transmite la información a terceros como si, en algunos casos, simplemente se accede ilegítimamente a los datos.

Existen muchísimos ejemplos en la práctica de sentencias que condenan al personal sanitario por este tipo de delitos. Por citar sólo algunos casos, pueden relacionarse los siguientes: STS, Sala 2ª, 4.4.2001 (RJ 2001/2016; MP: Andrés Martínez Arrieta), en la que se condena a una médico residente por divulgar información conocida con ocasión del acceso a la historia clínica de una paciente embarazada, en relación con dos interrupciones voluntarias del embarazo acaecidas con anterioridad; SAP Pontevedra, Sección 5ª, 5.5.2008 (JUR 2008/317830; MP: Victoria Eugenia Fariña Conde), que condena, en este caso, a un miembro del personal de gestión por acceder a más de 5.000 historias clínicas sin justificación[37]; STS, Sala 2ª, 18.10.2012 (RJ 2012/1437; MP: Juan Saavedra Ruiz), que condena a una enfermera por acceder a datos sobre la salud psiquiátrica de la pareja del ex marido de su hermana y transmitir a ésta dicha información para su utilización en sede judicial con el fin de solicitar la suspensión del régimen de visitas dispuesto a favor del padre; STS, Sala 2ª, 23.9.2015 (RJ 2015/4208; MP: Andrés Palomo del Arco), por la que se condena a un médico por acceder injustificadamente, hasta en 25 ocasiones, a las historias clínicas de sus compañeros de hospital[38]; o la STS, Sala 2ª, 3.2.2016 (Roj 185/2016; MP: Andrés Martínez Arrieta), condenatoria de un médico que accede hasta en 171 ocasiones a las historias clínicas de su ex pareja, enfermera del mismo hospital, y de la familia de ésta.

Vistos los ejemplos, parece clara la relevancia de estas conductas en el ámbito penal; lo cual no quiere decir que la práctica no haya suscitado alguna duda, como a continuación veremos.

c. La cuestión de la identidad del supuesto infractor y su conocimiento por el perjudicado

Aunque la lectura de los apartados precedentes podría no dar señales de ello, la defensa de los derechos de los afectados en los Tribunales puede llegar a presentar una complicación de orden práctico importante. Y es que, para poder ejercitar esta defensa, el perjudicado debe conocer, en primer lugar y como ya se ha dicho, que se ha dado un acceso ilegítimo a sus datos. Y, en segundo lugar, el dato sobre la identidad de las personas que hubiesen realizado los accesos tiene una importancia capital, como se verá.

[36] Debe resaltarse que, desde la reforma efectuada por la LO 1/2015, de 30 de marzo, modificativa del Código Penal, que introduce la responsabilidad penal de las personas jurídicas, pueden también las personas jurídicas ser responsables penalmente por el delito de descubrimiento y revelación de secretos según lo dispuesto por el artículo 197 quinques.

[37] A este respecto, es interesante traer a colación que el artículo 16.4 LAP dispone que el personal de gestión y administración puede acceder únicamente a los datos que sean imprescindibles para la prestación de los servicios en que consiste su trabajo.

[38] Que, en este contexto, son considerados pacientes a todos los efectos.

A este respecto, y al margen de la posibilidad extralegal de conocer el acceso a través de terceros, el Reglamento de desarrollo de la derogada LOPD[39] preveía en su artículo 103 lo que se conoce como registro de accesos, en el cual se preveía que se guardarían, de cada intento de acceso, "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". Sin embargo, y si bien había consenso en torno a que el derecho de acceso a la historia clínica, previsto en el artículo 15.1 LOPD (y, de manera más específica, en el artículo 18 LAP), incluía el de acceder al registro de los accesos efectuados a su historia clínica, no había acuerdo en torno a si este derecho incluía igualmente, o no, el de conocer las identidades de las personas concretas que habían accedido a los datos.

Pues bien, en torno al contenido exacto del derecho de acceso a la propia historia clínica según su regulación en la LOPD han existido durante los últimos años dos posiciones enfrentadas, que se augura pueden mantenerse tras la aprobación de la actual LOPDGDD. En primer lugar, la representada (principalmente) por la Agencia Española de Protección de Datos, que defiende que la revelación de la identidad de los supuestos infractores no se encuentra amparada por el derecho de acceso del artículo 15.1 LOPD. Destaca particularmente su Informe 167/2005, citado en multitud de resoluciones posteriores, algunas de ellas muy recientes[40], en el cual declara la AEPD, en un párrafo muy reproducido en posteriores pronunciamientos, que "el derecho concedido por la Ley únicamente abarcaría el conocimiento de la información sometida a tratamiento, pero no qué personas, dentro del ámbito de organización del responsable del fichero han podido tener acceso a dicha información", y ello por considerar, entre otras cuestiones, que la comunicación de dichos datos violentaría el propio derecho a la protección de datos de estas personas, debiendo contar para su transmisión, por tanto, bien con el consentimiento de dichas personas (lo cual parece improbable), bien con habilitación legal al respecto (la cual, según la Agencia, no se encontraría incluida en el derecho de acceso del art. 15.1 LOPD)[41]. En el mismo sentido se pronuncia la Agencia en ulteriores informes y resoluciones (Informe 171/2008 -también muy citado-, resolución R/01829/2009, y otros).

Esta misma corriente es seguida por la Agencia Vasca de Protección de Datos en su dictamen de 17 de mayo de 2011[42], con cita expresa del Informe de la AEPD 167/2005. También en sede

[39] Se trata del 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 (BOE núm. 17, de 19 de enero de 2008).

[40] Sólo a modo de ejemplo, porque son muy numerosas, pueden indicarse las siguientes resoluciones: R/01999/2017, R/02324/2017, R/02410/2017, R/02411/2017, R/03001/2017, R/00970/2018, RR/00342/2018.

[41] "La información reclamada en relación con las personas que hubieran conocido el contenido de la información de la consultante obrante en los ficheros de dicho Servicio debería ser considerada como datos de carácter personal, por lo que su revelación a la interesada, persona distinta del usuario, supondría una cesión o comunicación de datos, que debería contar con el consentimiento de aquel usuario o encontrarse habilitada por la Ley, lo que no sucedería en este caso, dado el alcance que la Ley Orgánica 15/1999 otorga al derecho de acceso".

[42] "CONCLUSIONES: 1. El ejercicio del derecho de acceso previsto en el artículo 15 de la LOPD incluye el derecho a conocer el número de accesos que se han producido a los datos de carácter personal de su titular, así como la finalidad del tratamiento que se está realizando. 2. El ejercicio del derecho de acceso previsto en el artículo 15 de la LOPD no incluye el derecho a conocer la identidad de los concretos usuarios que han accedido a sus datos objeto de tratamiento.".

jurisdiccional existen manifestaciones en este sentido, como la de la Sentencia de la Audiencia Nacional de 26 de febrero de 2014[43] (SAN, 26.2.2014 [Roj 936/2014; MP: Juan Pedro Quintana Carretero]), y otras que la citan, como la de 9 de febrero de 2018 (SAN 9.2.2018 [Roj 60/2018; MP: Fernando de Mateo Menéndez]), que además trata específicamente la cuestión del acceso indebido a la historia clínica y la petición del dato de los individuos que han podido acceder a la misma por parte del sujeto afectado, muy ilustrativa de la posición de la Audiencia en este tema; habiendo también muestras de esta tendencia en sede legislativa, de lo cual es ejemplo el artículo 19.2 del Decreto 24/2011, de 12 de abril, de la Documentación Sanitaria de Castilla-La Mancha (DOCM nº 74, de 15.4.2011)[44].

El Ministerio de Sanidad[45], por su parte, parece tomar un posicionamiento distinto al de la AEPD a través del Proyecto de Historia Clínica Digital en el Sistema Nacional de Salud[46]. El sistema que se pretende instaurar a través de este Proyecto, que se encuentra en diferentes fases de implementación en las Comunidades Autónomas[47], tiene como objetivo que los ciudadanos puedan ser atendidos en cualquier parte del territorio estatal con la garantía de que se dispone de su información clínica previa a través de la interoperabilidad de las historias clínicas entre los Servicios de Salud de las diferentes Comunidades Autónomas[48]. Y así, entre las diversas funcionalidades que dispone para los ciudadanos, se incluye la de poder acceder, precisamente, al Registro de los accesos efectuados sobre sus historias clínicas. Sin embargo, una vez se bucea un poco más en el Proyecto se aprecia cómo el texto, a pesar de llegar a tildar al ciudadano que hace uso de esta funcionalidad de auditor externo del sistema, no incluye la identidad de las personas

[43] Esta sentencia se dicta en un procedimiento en el que la demandante desea conocer si algún funcionario o miembro del personal administrativo del Ministerio de Hacienda y Administraciones Públicas podría haber accedido a sus datos fiscales personales de manera injustificada, produciéndose, además, una cesión de dichos datos a terceros. Dice la Audiencia en la sentencia que "debe destacarse que la solicitud de acceso a información formulada por la aquí reclamante (…) es ajena al contenido del derecho de acceso a datos personales que reconoce al titular de tales datos el artículo 15 de la LOPD, pues va dirigida a obtener información sobre la identidad de los funcionarios o servidores públicos que pudieran haber accedido a los datos personales de la actora, presumiendo que pudieran haberlos cedido a terceros. Por consiguiente, no tiene por objeto la obtención de información de sus datos de carácter personal sometidos a tratamiento, del origen de tales datos y de las comunicaciones realizadas o que se prevén hacer de los mismos por el responsable del fichero, sino acerca de los datos de identidad de aquellos empleados públicos pertenecientes a la organización administrativa del responsable del fichero que hubieran accedido a los mismos, que no quedan comprendidos en el derecho de acceso reconocido al titular de los datos personales y configurado legalmente en los términos expresados".

[44] La redacción de esta norma, además, podría dejar algunas dudas sobre los sujetos cuyas identidades protegería, toda vez que habla de las personas que hayan accedido "dentro del ámbito de organización del responsable del fichero" (véase, al respecto, GALLEGO RIESTRA y LIAÑO GALÁN, 2012, p. 88).

[45] Actualmente también de Consumo y Bienestar social, aunque hay que tener en cuenta que esta iniciativa comenzó a implantarse en el año 2006, bajo una diferente configuración ministerial.

[46] El texto del Proyecto puede consultarse aquí:

http://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf

[47] Véase al respecto el Informe de situación 1 de enero de 2019 consultable aquí:

https://www.mscbs.gob.es/gl/profesionales/hcdsns/contenidoDoc/WEB_Informe_de_Situacion_HCDSNS_Enero_2019.pdf

[48] Así se explica en la página web del Ministerio. La información puede consultarse aquí: https://www.mscbs.gob.es/gl/profesionales/hcdsns/contenidoDoc/Antec_e_historial.htm

que efectúan los accesos entre los datos sobre los que el interesado podría obtener información[49], por lo que se sitúa sin ambages en la línea marcada por la AEPD.

La posición contraria, por otro lado, defiende que dicho derecho se encuentra incluido en el derecho al acceso del art. 15.1 LOPD, y se ha visto plasmada ya en normativa autonómica como el artículo 31.1 de la Ley Foral 17/2010, de 8 de noviembre, de Derechos y Deberes de las Personas en materia de Salud en Navarra (BOE nº 315, de 28.12.2010), o el artículo 35 de la Ley 3/2005, de 8 de julio, de Información Sanitaria y Autonomía del Paciente (BOE nº 186, de 5.8.2005) de Extremadura. Esta postura ha sido defendida también por algunos organismos[50] y por buena parte de la doctrina, que, especialmente combativa en relación con este asunto, aporta argumentos como la falta de coherencia de la AEPD con la legislación vigente, y critica lo que parece ser un intento de configurar un inexistente derecho de aquellos profesionales que acceden de forma ilegítima a las historias clínicas a que no se desvele su identidad[51]; términos contundentes con los que, en suma, estamos de acuerdo.

---

[49] Dice el texto que el ciudadano dispondrá 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" (p. 16).

GALLEGO RIESTRA y LIAÑO GALÁN (2012, p. 87) critican, con razón, esta forma de proceder del Ministerio, diciendo que éste "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 renglón seguido, decir que no tienen derecho a saber quiénes concretamente han accedido legal o ilegalmente a sus datos de salud".

[50] El Grupo de Trabajo del Artículo 29 (que, se ha de recordar, es un órgano consultivo independiente que actúa en el ámbito supranacional, y, por tanto, formula sus propuestas de modo general y sin tener en cuenta las legislaciones particulares de los Estados) se posiciona también a favor de que los pacientes puedan obtener la información sobre quién ha accedido a su historial clínico, proponiendo, incluso, la remisión periódica a los mismos de los datos disponibles sobre dichos accesos, con inclusión expresa de las identidades de quienes hayan efectuado los accesos (documento WP131, p. 21).

Por otra parte, en el ámbito nacional, se alinea con esta posición el Informe SESPAS (pp. 65, 66), que no obstante indica que se requeriría una norma legal que previera dicho derecho (si bien nos parece que dicha *autorización* puede extraerse de la propia previsión legal del derecho de acceso, entendido con una amplitud algo mayor).

[51] Al respecto puede verse a GALLEGO RIESTRA y LIAÑO GALÁN, cuando dicen que no comprenden "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 [sic] 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" (2012, pp. 88, 89). Véase también GONZÁLEZ GARCÍA, 2014, pp. 279-281. GALLEGO RIESTRA, además, destaca el error en el que cae la AEPD al asimilar, en un primer momento, los profesionales que atienden a un paciente (los cuales, aportamos aquí, deben ser conocidos por el paciente en virtud del artículo 14.1 LAP y, también, como indica el autor, según la Ley de Ordenación de las Profesiones Sanitarias, que dispone al personal sanitario el deber de identificarse ante el paciente) con aquéllos que accedieron a su historia, para más tarde negar el derecho de conocer la identidad de estos últimos (2016, pp. 137-139).

Frente a estas manifestaciones contrasta el posicionamiento de TRONCOSO REIGADA, un tanto ecléctico, según el cual el derecho de acceso no implicaría conocer los posibles accesos que hubieran podido producirse a la historia clínica ya que "la información contenida en el registro de accesos excede del art. 15 LOPD" por no tratase de datos personales del afectado, por lo que no existe un deber legal al respecto y así "el paciente no tiene derecho a conocer el registro de accesos a su historia clínica", pese a lo cual reconoce que parece razonable introducir medidas, tales como el ofrecimiento de información sobre "el riesgo de accesos a sus datos personales", capaces de obtener un reequilibrio y compensar lo que el autor tilda de *injerencias* sobre el derecho fundamental a la protección de datos personales (2010, pp. 693, 694 y 1185).

Ciertamente, no parece lógico, ni conforme con la legislación vigente (téngase en cuenta, además, que el único límite expreso que el artículo 18.3 LAP establece al derecho de acceso con respecto a los derechos del personal sanitario es el relacionado con las anotaciones subjetivas), que se prive a los afectados de la posibilidad de conocer quién accede a sus datos, al tiempo que se ampara, más bien, al que accede ilegítimamente a los datos de terceros. No acaba de comprenderse, en fin, que se pongan tantas trabas a la entrega de esta información, teniendo en cuenta que la identidad de los profesionales que hayan accedido de manera justificada será ya, con toda probabilidad, conocida por el paciente, pudiendo sólo descubrir las identidades que hayan actuado de manera ilegítima, los cuales no parece que deban ser objeto de una protección especial por parte del Ordenamiento, más aún si ello puede condicionar la defensa de los derechos de los perjudicados ante los Tribunales.

Y es que la trascendencia de la cuestión puede apreciarse perfectamente al estudiar cómo, según la doctrina que ha tratado el tema[52], el desconocimiento de la identidad del supuesto infractor impediría la interposición de la denuncia del hecho en sede penal, toda vez que los delitos de descubrimiento y revelación de secretos son de carácter semipúblico y no pueden, por tanto, perseguirse de oficio. Así se indica en el artículo 201.1 CP, exceptuándose el caso de que el supuesto infractor sea autoridad o funcionario público, en cuyo caso sí podrá, en virtud de lo dispuesto por el apartado segundo del mismo artículo, procederse de oficio (claro que, en este último caso, el emprendimiento de acciones judiciales quedaría a expensas de que el responsable del fichero tuviera conocimiento de los hechos de algún modo y los trasladara a la autoridad judicial, quedando, así, la defensa de los derechos de los pacientes a expensas de la administración sanitaria[53]).

Sin embargo, parece conveniente matizar estas afirmaciones doctrinales por cuanto el desconocimiento de la identidad del supuesto infractor no tiene por qué implicar necesariamente la imposibilidad de denunciar y, por ende, de perseguir penalmente la actividad supuestamente delictiva, teniendo en cuenta que la inclusión del dato de la identidad del supuesto infractor sí es necesaria para la interposición de la querella pero no para la de la denuncia (véanse los arts. 270 y ss. y 259 y ss. CP, respectivamente), que es lo que procede en este tipo de delitos, según el artículo 201.1 CP.

Podría el perjudicado, por tanto, poner en conocimiento de las autoridades el hecho delictivo a través de la procedente denuncia sin necesidad de consignar la identidad del supuesto infractor, que podría averiguarse en la propia fase de instrucción del procedimiento penal[54].

[52] En particular, GALLEGO RIESTRA (2016, pp. 137-139).

[53] Como muy bien señala GALLEGO RIESTRA (2016, pp. 137-139).

[54] No es inimaginable que, en fase de instrucción, pudiera requerirse como prueba la declaración del responsable del fichero, o como prueba documental el propio registro de accesos al completo. Parece que apuntan a esto último GALLEGO RIESTRA y RIAÑO GALÁN (2012) cuando dicen que "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 (…)" (p. 80), si bien posteriormente se alinean de nuevo con el posicionamiento que defiende que no es posible abrir causa penal sin disponer de la información relativa a la identidad del infractor (p. 88).

Ahora bien, sí es cierto que, en tanto en cuanto no quede determinada la identidad del presunto responsable, no es posible abrir la fase de juicio oral, lo cual sin duda supone una complicación añadida y mayores dilaciones a la hora de perseguir este tipo de delitos y otorgar al afectado la tutela judicial que corresponde. Como también lo es, por otra parte, que con la última reforma de la Ley de Enjuiciamiento Criminal (aprobada por Real Decreto de 14 de septiembre de 1882, BOE nº 260, de 17.9.1882), en 2015, y la redacción dada a su artículo 284.2, las denuncias presentadas en sede policial por delitos cuyo autor sea desconocido podrían no llegar nunca a conocimiento del Ministerio Fiscal y de la autoridad judicial. Y ello porque, no tratándose de uno de los delitos de especial gravedad que recoge el artículo y que justificarían la remisión automática del atestado, sólo se prevé que éste se conserve "a disposición del Ministerio Fiscal y de la autoridad judicial, sin enviárselo", a menos que éstos soliciten la remisión o que la policía practique "cualquier diligencia después de transcurridas setenta y dos horas desde la apertura del atestado" y éstas tengan *algún resultado*. Como puede apreciarse, este artículo deja, como mínimo, dudas sobre la viabilidad de las denuncias de delitos sin autor identificado[55]; si bien no empece a la posibilidad de que el perjudicado presente la denuncia ante cualquiera de los otros organismos habilitados para ello, como el mismo artículo se encarga de recordar[56], por lo que no puede hablarse, verdaderamente, de una imposibilidad de denunciar en estos casos.

Con todo, y dejando a salvo las matizaciones referidas, es evidente que la denegación de acceso a la totalidad de los datos contenidos en el registro de accesos supone, como indica la doctrina referida, una cortapisa notable al ejercicio de los derechos de los afectados ante los Tribunales de la jurisdicción penal[57].

Sin embargo, donde el desconocimiento de la identidad de quien accedió injustificadamente sí es de importancia absoluta, a pesar de que la cuestión parece haber pasado sorprendentemente desapercibida para la práctica totalidad de la doctrina, es en el ordenamiento civil, al carecer éste de una fase de instrucción como la penal en la que se pueden extender diligencias de averiguación

[55] Es evidente que este artículo presenta importantes deficiencias de fondo y de forma que pueden dar lugar a grandes dificultades de interpretación. Así, por ejemplo, se prevé que el Ministerio Fiscal o la autoridad judicial puedan solicitar la remisión del atestado si las autoridades policiales no proceden a ello; pero ¿es posible, en ese caso, que el Ministerio Fiscal o la autoridad judicial lleguen siquiera a conocer la existencia de un atestado que no les ha sido remitido? O, por otra parte, y como otra de las circunstancias que motivarían la remisión del atestado a dichos cuerpos, ¿realmente es válida "cualquier diligencia" policial, o sólo contarían como tales las destinadas, en efecto, a descubrir la identidad del autor del delito? ¿Qué se entiende exactamente por "algún resultado"? ¿Cuál debería ser el grado de certeza del mismo? Sólo atendiendo a estas cuestiones, por no entrar en otras, queda patente que la redacción del artículo ofrece bien poca seguridad y claridad al asunto.

[56] Como solución ante el supuesto de que el atestado no fuera, finalmente, remitido a las autoridades correspondientes, lo único que prevé el artículo es que la víctima pueda reiterar la denuncia ante la fiscalía o el juzgado de instrucción (algo que, por otra parte, podría hacer el perjudicado como primera opción, quizás con mayor éxito o mayores garantías).

[57] Cosa distinta es que, una vez iniciado el procedimiento y de cara a la condena, la prueba aportada en relación a la identidad del supuesto infractor deba ser de suficiente entidad como para desvirtuar la presunción de inocencia. En este sentido se pronuncia la SAP Madrid, Sección 16ª, 13.3.2018 (ARP 2018/632), ya comentada, en la que el Tribunal indica que la huella digital que refleja una consulta de un profesional a una historia clínica acredita que se ha entrado con las claves de dicho profesional, pero no que sea éste quien efectivamente haya llevado a cabo ese acceso, remarcando en qué medida es importante en el ámbito penal, de cara a la destrucción del principio de presunción de inocencia, que la identidad del infractor quede suficientemente acreditada.

de la identidad del responsable del hecho dañoso. Así, será imposible interponer la debida demanda de reclamación de daños y perjuicios si no conocemos la identidad de la persona a la que queremos demandar, de tratarse de un particular.

Sí podría interponerse la demanda, no obstante, contra el centro sanitario privado (cuestión distinta es que se considerara responsable a la persona jurídica en el supuesto concreto), o contra el centro sanitario público, lo cual no ofrecería problema alguno, toda vez que el artículo 36.1 de la de la Ley de Régimen Jurídico del Sector Público faculta al particular para interponer la demanda directamente contra la Administración, sin perjuicio de una posterior repetición por parte de ésta contra el verdadero responsable del hecho dañoso. En estos dos supuestos, no obstante, el afectado debería saber, al menos, de qué centro sanitario concreto procede quien accedió indebidamente a su historia clínica.

En cualquier caso, no cabe duda de que, independientemente de la jurisdicción en la que nos situemos, la denegación de la revelación del dato de la identidad al perjudicado supone siempre, como mínimo, una obstaculización evidente a la adecuada defensa de los derechos de los perjudicados.

Estando así las cosas bajo la vigencia de la normativa anterior, ha de decirse que la cuestión sobre la posibilidad de conocer la identidad de quienes acceden a la historia clínica como parte del derecho de acceso del paciente se mantiene vigente con la nueva regulación del derecho de acceso, con independencia de que el registro de accesos se mantenga o no como medida[58]. Y ello porque el contenido específico del derecho de acceso, según aparece regulado en la nueva normativa, no parece distar mucho de la configuración que tenía bajo el imperio de la antigua Ley a estos efectos y, en cualquier caso, la norma no contiene cambio de criterio expreso alguno sobre este aspecto.

Así, puede apreciarse cómo el artículo 13 de la LOPDGDD indica que el derecho de acceso se ejercitará según lo dispuesto por el artículo 15 RGPD, el cual regula en su apartado primero la información que se considera incluida dentro del mismo. Pues bien, en la enumeración que realiza el artículo 15 no aparece la identidad de las personas pertenecientes a la empresa o entidad responsable de los datos que accedan a los mismos. Sí se incluye el derecho a conocer a los destinatarios de los datos (art. 15.c)), a los que el artículo 4.9 RGPD define como cualquier sujeto al que se comuniquen los datos, "se trate o no de un tercero". Sin embargo, esta previsión no se diferencia de los supuestos de cesión que ya contemplaba la antigua norma[59], los cuales ya se incluían en el derecho de acceso y no servían para justificar la petición de estos datos por parte de

[58] Se ha de recordar que el modelo que exponen tanto la LOPDGDD como el RGPD se basa en el principio de responsabilidad proactiva del responsable del tratamiento de los datos, que implica que se hayan de emplear las medidas de seguridad más adecuadas a cada caso, después de realizar un estudio del riesgo que supone el tratamiento concreto, sin que la Ley disponga niveles de seguridad distintos según el tipo de tratamiento, como hacía la normativa anterior. En todo caso, cabe la posibilidad de que allí donde los remedios adoptados hayan sido adecuados éstos se sigan manteniendo (véase CASANOVA ASENCIO, 2018, p. 6).

[59] La cesión o comunicación de datos se definía por el artículo 3.i) de la antigua LOPD como "toda revelación de datos realizada a una persona distinta del interesado".

los pacientes, entendiéndose así que en ellos no podían subsumirse los casos de acceso a la historia clínica del interesado por parte del personal sanitario[60].

Así, la nueva regulación no supondría cambio alguno, al comprender los mismos supuestos que hasta ahora se incluían en la LOPD, por lo que parece que la AEPD podría perfectamente mantener la interpretación hasta ahora realizada del derecho de acceso y la cuestión seguiría irresuelta, manteniéndose vigente la discusión expuesta.

Dejando al margen la posibilidad esbozada de conocer la identidad del infractor en virtud de un requerimiento judicial en fase de instrucción de un procedimiento penal[61], aún podría vislumbrarse otra posibilidad distinta para conocer este dato: se trataría del deber que el responsable del tratamiento tiene de comunicar al afectado la violación de la seguridad de sus datos (lo que se conoce como "brecha de seguridad"), en los términos dispuestos por el artículo 34 RGPD. Sin embargo, de considerarse esta obligación aplicable a este tipo de supuestos[62], el Reglamento no prevé que se comunique la identidad del infractor necesariamente; este dato no consta entre la información mínima imprescindible a comunicarse al interesado, por lo que, sin perjuicio de que en algún supuesto concreto pudiera comunicarse esta información, tampoco de este modo se resolvería el problema con carácter general.

En consecuencia, parece que el camino para obtener esta información, dadas las circunstancias estudiadas, habría de pasar por una reinterpretación del contenido del derecho de acceso en el

[60] No obstante, es interesante observar cómo la AEPD, en su Informe 171/2008, indica que los accesos justificados por la norma en virtud de los artículos 16 y 18 LAP son supuestos de cesión de datos, para a continuación dictaminar que el paciente no tiene derecho a conocer las identidades de quienes hubiesen accedido a la historia clínica, cosa que resulta francamente sorprendente si se tiene en cuenta que el derecho de acceso incluye literalmente el de conocer a los cesionarios de los datos (art. 15.1 de la antigua LOPD). Este posicionamiento de la AEPD resalta con respecto al modo de resolver de tantos otros pronunciamientos de la Agencia que tratan la cuestión y en los que no se indica en ningún momento que este tipo de usuarios (que, según la misma resolución, forman parte de la organización encargada del tratamiento de los datos) sean considerados como cesionarios. Supuesto en el cual, como ya se ha dicho y siguiendo lo dispuesto por la norma, se habría de conceder el derecho a conocer sus identidades, so pena de caer en la contradicción en la que incurre el Informe citado.

Comentando esta resolución, GALLEGO RIESTRA y RIAÑO GALÁN (2012) remarcan que además la AEPD identifica a los profesionales que accedieron con los que efectuaron el tratamiento, cuyos datos básicos de identificación tienen derecho a conocer los pacientes según lo dispuesto por el artículo 5.1.e) de la Ley de Ordenación de profesiones sanitarias, (pp. 84, 85). Además, para los autores citados la conceptualización de estos usuarios como cesionarios de los datos representa una posible vía para el paciente que desea conocer las identidades de los que acceden a sus datos (p. 88), aunque admiten dudas sobre si la Agencia realizaba estas afirmaciones de manera consciente o no (p. 84); conceptualización respecto de la cual caben las reservas que ya se han expresado.

[61] GALLEGO RIESTRA y RIAÑO GALÁN refieren también la posibilidad de conocer este dato a propósito de un procedimiento contencioso-administrativo (2012, p. 86).

[62] El artículo 34 RGDP dispone la obligatoriedad de notificar al afectado cuando la violación de los sistemas de seguridad de los datos pueda "entrañar un alto riesgo para los derechos y libertades de los titulares de los datos". La AEPD, por su parte, en uno de los varios documentos que en forma de Guías ha publicado a propósito de la entrada en vigor de la nueva normativa de protección de datos (en concreto, en su "Guía para la gestión y notificación de brechas de seguridad", pp. 42, 43), relaciona una serie de factores a tener en consideración con el fin de determinar si concurren estas circunstancias y si, en consecuencia, se ha de realizar la comunicación a las personas afectadas, según puede consultarse en el siguiente enlace: https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

sentido arriba apuntado, que permitiera soslayar los óbices y complicaciones que la falta de esta información presenta para los perjudicados.

d. El daño resarcible en materia de acceso indebido a la historia clínica

La LO 1/1982 prevé como intromisión ilegítima susceptible de generar responsabilidad civil, en su artículo 7.4, únicamente la filtración de los datos conocidos a propósito del desempeño de la actividad profesional.

Sin embargo, como puede extraerse de las sentencias citadas en los epígrafes precedentes, el mero acceso a los datos contenidos en la historia clínica, sin necesidad de que se produzca comunicación de los mismos a terceros, tiene ya consecuencias jurídicas. Cabe preguntarse, por tanto, si la conducta consistente en el mero acceso a los datos supone un daño indemnizable de por sí y también si, como sucede con las intromisiones ilegítimas recogidas por la LO 1/1982, es posible presumir la existencia de perjuicio, en aplicación analógica del artículo 9.3 de dicha Ley, el cual exime al perjudicado de la necesidad de desplegar actividad probatoria alguna relativa al daño sufrido una vez acreditada la intromisión ilegítima.

Del estudio de la jurisprudencia parece que, en efecto, el mero acceso supondría un hecho dañoso para el perjudicado, toda vez que los datos tienen el carácter de sensibles. Al menos, así se pronuncian diversas sentencias de la jurisdicción penal, donde los procedimientos por acceso indebido al historial clínico proliferan en mayor número[63], en las que se entiende que el mero acceso supone ya un perjuicio cuando se trate de datos de salud (como se indica en la muchas veces citada STS, Sala 2ª, 30.12.2009 (Roj 8457/2009; MP: Juan Ramón Berdugo Gómez de la Torre)[64], capaz de motivar, además de la condena por infracción del tipo penal correspondiente, la condena por responsabilidad civil derivada de delito, al considerarse, en sentencias como la STS, Sala 2ª,

[63] Aunque en materia de jurisprudencia es imposible estar completamente seguros, parece difícil encontrar sentencias del ámbito civil que condenen por el mero acceso a los datos de salud; tal vez, porque es posible que los afectados por este tipo de conductas ilícitas sean más proclives a encauzar sus reclamaciones a través de la vía penal, en la que, además de condenarse a la reparación del daño causado al perjudicado (reconociéndose expresamente la suficiencia del mero acceso a los datos para producir dicho perjuicio), se incluyen consecuencias de mayor calado para el infractor.

[64] En esta sentencia, el Tribunal manifiesta que el perjuicio que, según la jurisprudencia, debe concurrir en el mero acceso para configurar el tipo delictivo del artículo 197.2 CP (aunque el propio artículo requiera literalmente tan sólo el acceso) no debe ser probado cuando los datos a los que se accede son de carácter sensible, como ocurre con los datos sanitarios. Por otra parte, la SAP Cáceres, 5.12.2016 (ARP 1456; MP: Jesús María Gómez Flores), entre otras que podrían citarse, es muy clara al decir, incluyendo una referencia al derecho constitucionalmente reconocido a la intimidad, que "no se exige la acreditación de perjuicio alguno ya que el mero acceso constituye un perjuicio para el titular porque se está vulnerando su derecho constitucional a la intimidad". Aunque esta apreciación se hace en relación a los elementos configuradores del tipo penal, es de relevancia por cuanto la incursión o no en el tipo penal es determinante a la hora de desprenderse una responsabilidad civil en dicha instancia.

3.2.2016 (Roj 185/2016)[65]; SAP Cáceres, 5.12.2016 (ARP 2016/1456)[66]; o SAP Navarra, 3.4.2017 (Roj SAP NA 197/2017; MP: Ricardo Javier González González)[67], que las conductas descritas en los hechos probados provocaban un daño moral innegable a los perjudicados, como consecuencia directa y natural de los hechos[68].

Por tanto, a diferencia de lo que ocurre en relación con las intromisiones ilegítimas del artículo 7.4 LO 1/1982, no es precisa en estos casos la difusión para que se aprecie un daño; y, si bien no parece que el artículo 9.3 de la misma Ley se aplique analógicamente de manera que el daño se presuma expresamente, lo cierto es que, al menos en la totalidad de los casos estudiados, los Tribunales sí parecen considerar que el daño es consecuencia natural de los hechos probados, y que éste se da por el mero acceso a los datos, el cual ya supone un perjuicio que no precisa de mayor prueba.

Evidentemente, lo dicho no es óbice para que pueda estimarse un daño mayor cuando, además de darse un simple acceso a los datos protegidos, éstos sean difundidos, como ocurre en la STS, Sala 1ª, 27.1.1997 (Roj 452/1997), antes citada, en la que, por cierto, tampoco se recurre a la vía del artículo 7.4 LO 1/1982, sino que se condena en virtud de los artículos 1902 y 1903 CC.

Aún más, en materia de valoración del daño cabría preguntarse si no serían de aplicación los criterios que la misma LO 1/1982 dispone para la cuantificación del daño moral en su artículo 9.3. Sin embargo, y siguiendo la línea de pensamiento ya esgrimida, no parece que puedan ser de aplicación, toda vez que dichos criterios están previstos para una intromisión consistente en la difusión de los datos personales, y, coherentemente, se incluye entre éstos "la audiencia o difusión del medio" a través del que dicha intromisión se haya producido; cuestión distinta es que el juzgador pueda acudir a los otros criterios dispuestos en el artículo (a saber, las circunstancias del caso y la lesión efectivamente producida), que, de todas formas, no dejan de ser criterios generales de valoración del daño.

---

[65] En esta sentencia, antes referenciada, se confirma la condena a un médico por acceder hasta en 171 ocasiones al historial clínico de su ex pareja y de diversos familiares de ésta. Aunque la sentencia del Tribunal Supremo no entra en la cuestión de fondo relativa a la responsabilidad civil, sí lo hace la de la Audiencia (SAP Baleares, 28.1.2015 [JUR 79385; MP: Alberto Jesús Rodríguez Rivas]), que condena por daños morales basándose, para el cálculo de la cuantía indemnizatoria, en el Baremo contenido en el Anexo del Texto Refundido de la Ley sobre Responsabilidad Civil y Seguro en la Circulación de Vehículos a Motor, práctica habitual de los Tribunales, como se sabe, para la determinación del monto indemnizatorio.

[66] En esta sentencia, en la que se condena a una enfermera por acceder a las historias clínicas de dos facultativos de su mismo centro de trabajo, que son padre de los nietos de la acusada y pareja de éste, respectivamente, dice el Tribunal al enjuiciar la responsabilidad civil dimanante del delito que "comportamientos como los enjuiciados, en los términos expuestos de continuidad, intensidad y reiteración, así como el carácter sensible de los datos y la información comprometida han producido un innegable impacto emocional y el consiguiente perjuicio a las víctimas", si bien también tiene en cuenta el hecho de que no se ha producido difusión ninguna de dichos datos reservados al evaluar las indemnizaciones.

[67] Sentencia en la que se condena a una enfermera por acceder injustificadamente, en múltiples ocasiones, a los historiales clínicos de su ex pareja y de otras personas relacionadas con éste.

[68] La SAP Cáceres, 5.12.2016 (ARP 2016/1456) argumenta, con cita de reiterada jurisprudencia del Tribunal Supremo, que el perjuicio "no necesita estar especificado en el relato de los hechos probados cuando fluye de manera directa y natural del referido relato histórico, por lo que el daño moral no necesita de prueba cuando se infiera de manera inequívoca de los hechos".

Puede decirse, por último, que el hecho de que el simple acceso a los datos se considere una conducta antijurídica capaz de fundamentar, además de un tipo delictivo concreto, una condena por los daños causados, en comparación con el contenido de la LO 1/1982, según la cual sólo la difusión es constitutiva de una intromisión ilegítima capaz de generar responsabilidad, es clara muestra de la evolución acaecida en la materia y de cómo el legislador ha adquirido en las últimas décadas mayor conciencia de las implicaciones que la toma de conocimiento de estos datos particularmente sensibles supone.

3.3. Procedimiento arbitral específico en materia de historia clínica y datos de salud

El Grupo de Trabajo del Artículo 29 propone, como posible nuevo mecanismo a implementar por los Ordenamientos jurídicos de los Estados miembros, la posibilidad de adoptar un sistema de arbitraje en materia de uso y tratamiento de los datos contenidos en la historia clínica electrónica, con el objetivo de otorgar a los afectados un procedimiento fácilmente accesible y gratuito, en el que, según se indica en el documento[69], habrían de actuar profesionales con experiencia médica incluso con preferencia a las autoridades en protección de datos. Esta solución podría ser cuestionada en el sentido de que, si bien también sería precisa la intervención de expertos en materia sanitaria con el fin de determinar, sobre todo, el cumplimiento del principio de proporcionalidad en el acceso (es decir, que se accede a aquella información necesaria para la prestación de la adecuada asistencia sanitaria), probablemente la participación de las autoridades de protección de datos habría de configurarse como preponderante, siendo que la resolución de las disputas pasaría, principalmente, por la aplicación del derecho de protección de datos, más que por consideraciones de tipo médico.

Si bien la implementación de esta solución como una opción más para el perjudicado podría evitar en algunos casos el recurso a la siempre más costosa (en varios sentidos) vía judicial, sería preciso estudiar si la incidencia de este tipo de reclamaciones justifica la creación de un procedimiento arbitral *ad hoc*, cuál sería su configuración exacta, en su caso, y si no hay otras cuestiones en esta materia que requieren de una atención más urgente, como la resolución de la controversia relacionada con la identidad del supuesto infractor, por ejemplo.

Cosa distinta es la que se dispone en la nueva normativa de protección de datos personales, al regularse los códigos de conducta en los artículos 40 y siguientes del Reglamento, los cuales se prevé que puedan contener especificaciones relacionadas sobre la resolución extrajudicial de conflictos (no necesariamente un procedimiento arbitral específico), como expresamente contempla el artículo 38.1 LOPDGDD, y que podrían ser útiles, en su caso, para evitar la sustanciación de la controversia en vía judicial.

[69] Documento WP131, p. 21.

3.4. Sanciones deontológicas por vulneración del deber de secreto profesional

Dependiendo del texto de los Estatutos de cada Colegio Profesional, la vulneración de este deber puede ser considerada falta entre grave y muy grave, acarreando consecuencias que llegan hasta la inhabilitación profesional[70].

Una vez se reseña esta posibilidad como posible consecuencia de la infracción de los deberes de confidencialidad del personal sanitario, no deja de ser pertinente decir que la imposición de este tipo de sanciones por parte de los Colegios Profesionales (si bien prácticamente inexistente en la práctica) suscita algunas dudas, siendo que sanciones como la inhabilitación profesional se asimilan, más bien, a penas propias del Ordenamiento penal, pero impuestas no por el juez predeterminado por la ley en el seno de un procedimiento judicial con todas las garantías, sino por un Tribunal profesional (y hay que recordar que la Constitución Española prohíbe los tribunales de honor en el ámbito de la Administración civil y de las organizaciones profesionales en su artículo 26) y sin haberse cometido delito alguno de los previstos en el Código Penal.

Cuestión distinta es, evidentemente, que, paralelamente al procedimiento disciplinario llevado a cabo a propósito de la falta deontológica, se dé curso a un procedimiento penal por haber incurrido el profesional en uno de los delitos de los artículos 197 y siguientes del Código Penal, antes comentados. Lo que aquí se comenta es que los Estatutos de los Colegios Médicos permitirían a dichos Colegios imponer una sanción que, de tener verdaderos efectos *ad extra*, tendría las mismas consecuencias que una verdadera pena, y ello sin darse las garantías propias del procedimiento penal ni existir habilitación legal alguna que respalde una potestad sancionadora en la que no interviene la autoridad judicial.

El hecho de que la sanción impuesta pueda o no tener efectos en el ámbito externo al Colegio Profesional es relevante, y va a depender de que la colegiación se entienda o no como obligatoria. Y es que, de no ser obligatoria, las sanciones impuestas por el Colegio Profesional realmente no tendrían virtualidad alguna en el ámbito *extracolegial*, porque, a pesar de que la sanción de separación colegial pudiera tener el efecto interno de que el expulsado no pudiera ya formar parte de dicha organización, ésta no dejaría de ser una asociación de afiliación voluntaria y, con ello, la condición de asociado no sería imprescindible para el ejercicio de la profesión. Sin embargo, si la colegiación fuera obligatoria, y, por tanto, las sanciones tuvieran un verdadero efecto traspasado el ámbito colegial, sí se estaría impidiendo al profesional ejercer su profesión, y ello sin existir precepto legal que respaldara la sanción (se violaría, por tanto, el principio de legalidad) ni un procedimiento con todas las garantías, lo cual sería de dudosa constitucionalidad.

Por tanto, parece que, o la colegiación no es obligatoria y, por tanto, la sanción no puede tener verdaderos efectos más allá del ámbito del Colegio profesional, o, si lo es, se estaría incurriendo en inconstitucionalidad al no haber precepto legal que respalde la imposición de una sanción de este

[70] Así lo hacen, por ejemplo, los Estatutos de los Colegios de Médicos de Cádiz, A Coruña, Barcelona, Murcia, Madrid, Valencia y otros, todos en términos muy similares.

tipo con verdaderos efectos *ad extra*[71]. Añádase también que la propia constitucionalidad de una colegiación obligatoria lleva años siendo cuestionada por la doctrina[72].

4. Conclusiones

La historia clínica se compone de un conjunto de datos que deben ser protegidos adecuadamente, toda vez que se trata de datos especialmente vulnerables y en estrecha conexión con la intimidad de la persona. Al mismo tiempo, se trata de un instrumento absolutamente necesario para el desarrollo de la asistencia sanitaria por parte del personal sanitario; lo que determina que debe garantizarse el acceso de estos profesionales al mismo sin que con ello se provoque perjuicio alguno sobre el derecho a la intimidad y a la protección de los datos personales de los pacientes, los cuales puede verse afectado todavía con mayor incidencia con la implantación de los nuevos sistemas de historia clínica electrónica.

Así, es de vital importancia poder disponer de criterios que nos permitan distinguir con claridad cuándo un acceso está justificado y cuándo no lo está, y para ello contamos con varios principios

[71] A esta conclusión llega MACANÁS VICENTE (2017, pp. 2-4) en una obra dedicada al deber de colegiación para el ejercicio de la abogacía, pero que nos parece perfectamente aplicable, en su parte general, al supuesto que nos ocupa. Según indica el autor, reiterada doctrina constitucional parece contraria a un deber de colegiación general, al tiempo que todas las normas que estipulan un deber de colegiación para el ejercicio de una profesión lo sujetan a la condición de que así lo establezca una ley estatal. Así lo hacen el artículo 3 de la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales (BOE nº 40, de 15.2.1974), tras la reforma efectuada por la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio (BOE nº 308, de 23.12.2009) (conocida como "Ley Ómnibus"); el artículo 3 de la propia Ley 17/2009, sobre el libre acceso a las actividades de servicios y su ejercicio (BOE nº 283, de 24.11.2009) (conocida como "Ley Paraguas"); y también el artículo 4.8.a) de la Ley 44/2003, de 22 de noviembre, de ordenación de las profesiones sanitarias (BOE nº 280, de 22.11.2003) que hace, además, una mención expresa a la potestad sancionadora de los Colegios Profesionales en su apartado c) que nuevamente se hace depender de la previsión legal de dicha obligación de colegiación. Acaso la única ley estatal que podría avalar una colegiación obligatoria sería la propia Ley de ordenación de las profesiones sanitarias, cuando, al definir las profesiones sanitarias tituladas en su artículo 2, dice que son aquéllas que, entre otras cuestiones, "están organizadas en colegios profesionales oficialmente reconocidos por los poderes públicos" (apartado primero). Sin embargo, no queda claro si lo que la norma hace es tanto imponer la colegiación para estos profesionales, cuanto presuponerla, y parece que si de limitar un derecho fundamental se trata (la vertiente negativa del derecho de asociación), esta previsión debería ser, cuando menos, lo más clara posible, si es que no debiera hacerse a través de los cauces de una Ley Orgánica. Puede ser útil recordar en este punto que la Disposición transitoria cuarta de la Ley Ómnibus emplazaba al Gobierno para presentar un Proyecto de Ley que habría de determinar las profesiones para cuyo ejercicio fuera obligatoria la colegiación; previsión que habría clarificado la situación y a la que, desafortunadamente, no se dio cumplimiento.

Cuestión distinta, por otra parte, es que la colegiación siga siendo obligatoria en los casos concretos en los que ya lo fuera en tanto en cuanto no se publique ley estatal al respecto, como indica la misma Disposición transitoria cuarta. El Tribunal Supremo, hace, precisamente, aplicación de esta previsión en su STS, Sala 3ª, 16.7.2018 (RJ 2018/3563; MP: Octavio Juan Herrero Pina), para ratificar la legalidad de la colegiación de oficio efectuada por el Colegio de Protésicos Dentales de la Comunidad Valenciana, toda vez que la Ley 2/2000, de 31 de marzo, de creación del Colegio Oficial de Protésicos Dentales (BOE nº 94, de 19.4.2000) de la Comunidad Valenciana exigía la colegiación obligatoria, pero de ello no se puede derivar, en ningún caso, una obligatoriedad general de colegiación para las profesiones sanitarias.

Parece, por tanto, que es necesaria en esta materia una ley estatal que de manera clara, expresa y directa establezca la obligatoriedad de la colegiación para el ejercicio de aquellas profesiones para las que la misma se considere oportuna, si quieren evitarse ulteriores controversias al respecto.

[72] ATAZ LÓPEZ apuntaba, ya en 1985, a una posible inconstitucionalidad de la obligación de colegiación para el ejercicio de la profesión de médico (1985, pp. 50, 51, nota 40).

(señaladamente, el de vinculación asistencial y el de confidencialidad) cuya aplicación permite determinar en qué casos el acceso es legítimo, así como con el deber general de confidencialidad que, como pilar básico en la materia, debe regir toda relación entre el personal sanitario y el paciente.

Sin embargo, y aunque el objetivo primordial en este ámbito debe ser la evitación de cualquier acceso ilegítimo (especialmente con la aprobación de la nueva legislación en materia de protección de datos, que hace hincapié en la seguridad de los mismos), la práctica demuestra que neutralizar por completo este tipo de actuaciones es materialmente imposible. Así las cosas, han de arbitrarse procedimientos que permitan actuar frente a dichos accesos injustificados.

Entre todas las consecuencias presentadas, es particularmente interesante la relacionada con la defensa de los derechos de los perjudicados frente a los Tribunales, que, como se ha visto, puede llevarse a cabo a través de diversos cauces procesales, y que presenta no pocas cuestiones a resolver, aun con la nueva normativa de protección de datos referida.

Y si la nueva legislación presenta dudas, ello es señal de que todavía quedan avances por realizar en esta materia, lo cual no es extraño dadas sus particulares características, que determinan que, a la hora de regular esta materia, puedan apreciarse un conflicto entre diversos derechos (por ejemplo, el de la intimidad y el de la salud, ambos del paciente[73], o el derecho a la protección de los datos personales del paciente frente a este mismo derecho del profesional[74]).

En definitiva, puede decirse que lo relevante en esta materia es conseguir orquestar un sistema que sea, al menos, capaz de otorgar al usuario (en este caso, los pacientes) garantías suficientes en cuanto a su buen funcionamiento; y que, si bien es imposible asegurar de manera absoluta la ausencia de accesos injustificados a los datos, por la propia naturaleza de los ficheros y del uso al que sirven, sí disponga el sistema una serie de consecuencias que, a modo de resortes a los que acudir una vez acaecida la violación, se configuren como remedios que permitan a los afectados defender sus derechos, así como al propio sistema reaccionar frente a prácticas ilegítimas que, a la postre, vienen a menoscabar la credibilidad del sistema de salud en su conjunto.

Por tanto, se ha de seguir avanzando en el tratamiento de una materia en la que, si bien se han dado importantes avances en los últimos años –como el RGPD y la LOPDGDD demuestran- todavía presenta muchos puntos oscuros que deben ser esclarecidos.

[73] Véase TRONCOSO REIGADA, quien aboga por la búsqueda de un equilibrio entre los distintos derechos en juego a través del principio de proporcionalidad (2006, p. 49).

[74] Así, por ejemplo, cuando se habla de la posibilidad de configurar un derecho del paciente a conocer las identidades de aquéllos que acceden a sus datos.

5. Tabla de jurisprudencia citada

Tribunal Constitucional

Resolución y fecha	*Referencia*	*Magistrado Ponente*
Auto, 11.12.1989	RTC 1989/600	*Desconocido (magistrados: Miguel Rodríguez-Piñero y Bravo-Ferrer, Antonio Truyol Serra y Álvaro Rodríguez Bereijo)*
STC, 14.2.1992	RTC 1992/20	*Francisco Tomás y Valiente*
STC, 20.7.1993	RTC 1993/254	*Fernando García-Mon y González Regueral*

Tribunal Supremo

Resolución y fecha	*Referencia*	*Magistrado Ponente*
STS, Sala 1ª, 27.1.1991	Roj 452/1997	*José Almagro Nosete*
STS, Sala 2ª, 4.4.2001	RJ 2001/2016	*Andrés Martínez Arrieta*
STS, Sala 2ª, 30.12.2009	Roj 8457/2009	*Juan Ramón Berdugo Gómez de la Torre*
STS, Sala 2ª, 18.10.2012	RJ 2013/1437	*Juan Saavedra Ruiz*
STS, Sala 2ª, 23.9.2015	RJ 2015/4208	*Andrés Palomo del Arco*
STS, Sala 2ª, 3.2.2016	Roj 185/2016	*Andrés Martínez Arrieta*
STS, Sala 2ª, 4.7.2016	RJ 2016/2856	*Manuel Marchena Gómez*
Auto TS, Sala 2ª, 13.9.2018	JUR 2018/300037	*Manuel Marchena Gómez*
STS, Sala 2ª, 23.10.2018	RJ 2018/4717	*Luciano Varela Castro*
STS, Sala 3ª, 16.7.2018	RJ 2018/3563	*Octavio Juan Herrero Pina*

Audiencia Nacional

Resolución y fecha	*Referencia*	*Magistrado Ponente*
SAN, 26.2.2014	Roj SAN 936/2014	*Juan Pedro Quintana Carretero*
SAN, 9.2.2018	Roj SAN 60/2018	*Fernando de Mateo Menéndez*

Tribunal Superior de Justicia

Resolución y fecha	*Referencia*	*Magistrado Ponente*
STSJ Navarra, Sala de lo Contencioso-Administrativo, Sección 1ª, 8.2.2012	RJCA 2012/143	*Antonio Rubio Pérez*

Audiencias Provinciales

Tribunal, resolución y fecha	*Referencia*	*Magistrado Ponente*
SAP Pontevedra, Sección 5ª, 5.5.2008	JUR 2008/317830	*Victoria Eugenia Fariña Conde*
SAP Baleares, 28.1.2015	JUR 2015/79385	*Alberto Jesús Rodríguez Rivas*
SAP Cáceres, 5.12.2016	ARP 2016/1456	*Jesús María Gómez Flores*
SAP Navarra, 3.4.2017	Roj SAP NA 197/2017	*Ricardo Javier González González*
SAP Madrid, Sección 16ª, 13.3.2018	ARP 2018/632	*Francisco David Cubero Flores*
SAP A Coruña, Sección 6ª, 8.10.2018	JUR 2018/314374	*César González Castro*

6. Bibliografía

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Informes Jurídicos 167/2005, 171/2008 y Resoluciones R/01829/2009, R/01999/2017, R/02324/2017, R/02410/2017, R/02411/2017, R/03001/2017, R/00970/2018 y RR/00342/2018.

-(2018), *Guía para la gestión y notificación de brechas de seguridad*. Disponible en: https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf (Fecha de última consulta: 8.1.2019).

AGENCIA VASCA DE PROTECCIÓN DE DATOS, Dictamen de 17 de mayo de 2011. Disponible en: http://www.avpd.euskadi.eus/contenidos/dictamen_avpd/d11_025/es_def/adjuntos/CN11-009_DIC_D11-025.pdf (Fecha de última consulta: 2.12.2018).

Cecilia ÁLVAREZ RIGAUDIAS (2016), "Tratamiento de datos de salud", en María ÁLVAREZ CARO (coord.), Miguel RECIO GAYO (coord.) y José Luis PIÑAR MAÑAS (dir.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, pp. 171-186.
Joaquín ATAZ LÓPEZ (1985), *Los médicos y la responsabilidad civil*, Ed. Montecorvo, Madrid.

Inmaculada BARRAL (2011), "Datos relativos a la salud e historia clínica: la confidencialidad de los datos médicos", en María Rosa LLÁCER MATACÁS, *Protección de datos personales en la sociedad de la información y la vigilancia*, La Ley, Madrid, pp. 352-368.

Andrea Salud CASANOVA ASENCIO (2018), "Mecanismos de prevención del acceso indebido a la historia clínica por parte del personal sanitario y nueva legislación de protección de datos", *Bioderecho.es: Revista internacional de investigación en Bioderecho*, nº 7, 2018.

COMISIÓN CENTRAL DE DEONTOLOGÍA DE LA ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA y la COMISIÓN PERMANENTE DEL CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS (2017), *Decálogo de la Historia Clínica*. Disponible en: http://www.comalmeria.es/sites/default/files/noticias/docs/decalogo_sobre_historia_clinica.pdf (Fecha de última consulta: 20.10.2018).

CONSELLO DE BIOÉTICA DE GALICIA (2017), *Ética en el acceso y en el uso de la documentación clínica: reflexiones y recomendaciones*. Disponible en: https://extranet.sergas.es/catpb/Docs/cas/Publicaciones/Docs/AtEspecializada/PDF-2669-es.pdf (Fecha de última consulta: 12.10.2018).

María Nieves DE LA SERNA BILBAO y Fernando FONSECA FERRANDIS (2017), "El acceso a la historia clínica; el alcance del derecho", en Luciano José PAREJO ALFONSO (coord.) y José VIDA FERNÁNDEZ (coord.), *Los retos del Estado y la Administración del siglo XXI: libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo*, vol. 2, tomo 2, Tirant lo Blanch, Madrid, pp. 2271-2320.

Noelia DE MIGUEL SÁNCHEZ (2002), *Secreto médico, confidencialidad e información sanitaria*, Marcial Pons, Madrid.

Javier ETREROS HUERTA (2009), "Historia clínica electrónica", en Rafael CÁLIZ CÁLIZ (coord.), *El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica*, Thomson Reuters-Aranzadi, Cizur Menor, pp. 181-200.

Sergio GALLEGO RIESTRA (2016), "Los derechos de acceso, rectificación, cancelación y oposición del paciente sobre su historia clínica", *Derecho y Salud*, vol. 26, nº extra 1, pp. 133-140.

Sergio GALLEGO RIESTRA e Isolina RIAÑO GALÁN (2012), "¿Tiene el paciente derecho a saber quiénes y por qué han accedido a su historia clínica?", *Derecho y Salud*, vol. 22, nº 1, pp. 79-89.

Cristina GÓMEZ PIQUERAS (2009), "La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos", en Rafael CÁLIZ CÁLIZ (coord.), *El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica*, Thomson Reuters-Aranzadi, Cizur Menor, pp. 127-160.

Lola GONZÁLEZ GARCÍA (2014), "Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos", *Derecho y Salud*, vol. 24, nº extra 1, pp. 274-285.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2007), Documento WP131, de 15 de febrero. Disponible en: https://www.apda.ad/sites/default/files/2018-10/wp131_es.pdf (Fecha de última consulta: 8.1.2019).

Gabriel MACANÁS VICENTE (2017), ¿Existe un deber de colegiación para el ejercicio de la abogacía?, *Diario La Ley*, nº 9071.

Rafael Álvaro MILLÁN CALENTI (2013), "Historia clínica electrónica: accesos compatibles", en David LARIOS RISCO (coord.), *Tratado de Derecho Sanitario*, vol. 1: vol. I, Thomson Reuters-Aranzadi, Cizur Menor, pp. 779-802.

MINISTERIO DE SANIDAD, *El sistema de Historia Clínica Digital del Sistema Nacional de Salud*. Disponible en: http://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf (Fecha de última consulta: 3.1.2019)

-(2019), *Informe de situación de enero de 2019*. Disponible en: https://www.mscbs.gob.es/gl/profesionales/hcdsns/contenidoDoc/WEB_Informe_de_Situacion_HCDSNS_Enero_2019.pdf (Fecha de última consulta: 3.1.2019).

Marta ORDÁS ALONSO (2016), "Intimidad, secreto médico y protección de datos sanitarios", en Juan Antonio García Amado, *Razonar sobre Derechos*, Tirant lo Blanch, Valencia, pp. 773-834.

Patricia PALACIOS PALACIOS, y Marta ESCUDERO GONZÁLEZ (2011), "Protección de datos en el sector sanitario: el acceso a la historia clínica", en Ana I. HERRÁN (coord.), *Derecho y nuevas tecnologías*, Vol. 1, Universidad de Deusto, Bilbao, pp. 265-274.

Mar PEREIRA ÁLVAREZ (2009), "El tratamiento de los datos en las HCE y las medidas de seguridad: una aproximación desde el punto de vista técnico. Especial Referencia al nuevo Reglamento de desarrollo de la LOPD", en Rafael CÁLIZ CÁLIZ (coord.), *El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica*, Thomson Reuters-Aranzadi, Cizur Menor, pp. 305-320.

Javier SÁNCHEZ CARO (2009), "La historia clínica gallega: un paso importante en la gestión del conocimiento", *Derecho y salud*, vol. 18, nº 1, pp. 57-86.

María Mercedes SERRANO PÉREZ (2013), "Salud pública, epidemiología y protección de datos", en David LARIOS RISCO (coord.), *Tratado de Derecho Sanitario*, vol. 2: vol. II, Thomson Reuters-Aranzadi, Cizur Menor, pp. 1091-1113.

SOCIEDAD ESPAÑOLA DE SALUD PÚBLICA Y ADMINISTRACIÓN SANITARIA (SESPAS) (2017), *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*. Disponible en: http://sespas.es/2017/11/30/proteccion-de-datos-personales-y-secreto-profesional-en-el-ambito-de-la-salud-una-propuesta-normativa-de-adaptacion-al-rgpd/ (Fecha de última consulta: 10.10.2018).

Antonio TRONCOSO REIGADA (2006), "La confidencialidad de la historia clínica", *Cuadernos de Derecho Público*, nº 27, enero-abril, pp. 45-14.

-(2010), *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia.