MARCO NORMATIVO DE LA HISTORIA CLÍNICA ELECTRÓNICA Y SU INCIDENCIA EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

ANDRÉS FELIPE CONTRERAS P.*

RESUMEN

Como se esperaba desde hace algunos años, las ventajas del uso de sistemas de información no tardarían en incubar su legado en un sector tan relevante como lo es el de la prestación de servicios de salud y la forma en que se garantiza la eficiencia de dicha oferta de servicio en un ámbito tanto personal como social.

Bajo esta idea, en Colombia se expide en 2020 la Ley 2015, mediante la cual se crea la historia clínica electrónica interoperable. Tal reglamentación pretende facilitar, agilizar y garantizar el acceso y ejercicio de los derechos a la salud y a la información de las personas con la implementación de un diseño de interoperabilidad que propende a sistematizar los datos clínicos y asistenciales de los pacientes, permitiendo, para permitir, entre otras cosas, la trazabilidad, confidencialidad e integridad de dicha información, relacionan directamente con la privacidad e intimidad de los pacientes.

Palabras clave: historia clínica, *habeas data*, paciente, intimidad, interoperabilidad.

* Abogado de la Universidad Externado de Colombia, especialista en Responsabilidad y Daño Resarcible de esta misma casa de estudios. Becario en el programa de Maestría en Protección de Datos Personales de la Universidad Internacional de La Rioja. Experto en derecho informático y aspectos jurídicos de las tecnologías disruptivas (Bogotá). Contacto: andres.contreras@uexternado.edu.co. Fecha de recepción: 11 de febrero de 2020. Fecha de aceptación: 26 de marzo de 2020. Para citar el artículo: Contreras P., Andrés Felipe. Marco normativo de la historia clínica electrónica y su incidencia en el ámbito de la protección de datos personales en Colombia. *Revista La Propiedad Inmaterial* n.º 29, Universidad Externado de Colombia, enero-junio, 2020, pp. 95-116. DOI: https://doi.org/10.18601/16571959.n29.04.

REGULATORY FRAMEWORK OF THE ELECTRONIC MEDICAL RECORD AND ITS INCIDENCE IN THE FIELD OF PERSONAL DATA PROTECTION IN COLOMBIA

ABSTRACT

As has been expected for the past several years, it would not be long before the advantages of information systems would soon be reflected in the health services sector, including the manner in which the efficiency of such sector is guaranteed both at personal and social levels. Under this idea, Law 2015 of 2020 was passed in Colombia. This law creates the interoperable clinic history, seeking to facilitate and guarantee the access and exercise of the rights to health and information of individuals. It implements an interoperability design, in an effort to systematize clinical and healthcare data of patients, thereby allowing, among other things, the traceability, confidentiality and integrity of information directly related to the privacy and intimacy of patients.

Keywords: clinical history, *habeas data*, patient, privacy, interoperability.

INTRODUCCIÓN

El 31 de enero de 2020 se expide en Colombia la Ley 2015 de 2020 que crea la denominada *historia clínica electrónica interoperable*, la cual tiene como principal objetivo el regular el intercambio de datos clínicos relevantes, así como los documentos y expedientes clínicos de cada persona en correlativa defensa de su derecho a la salud y a la información, y ajustado todo ello al ejercicio de su derecho fundamental de *habeas data*.

Con ocasión de la expedición de dicha norma, el presente escrito tiene como objeto verificar cómo en materia sanitaria se puede dar la adecuada adaptación de las empresas de este sector al contexto de la historia clínica electrónica interoperable, con sujeción a la normativa aplicable en materia de protección de datos personales en Colombia y otras normas que regulan concretamente la documentación sanitaria resumida en la historia clínica. Se pretende entonces presentar dicho contexto, junto con algunos retos y ventajas que se plantean en el ámbito de la privacidad y protección de datos personales de los pacientes, en contraste con las obligaciones puntuales que tienen las entidades e instituciones de salud en la actualidad. La metodología para implementar será la presentación del marco de fuentes primarias, tales como son las normas que regulan el asunto en la Unión Europea (especialmente, España) y en Colombia, así como fuentes secundarias que se basan en análisis jurisprudenciales locales e internacionales y doctrina compacta y reconocida en la materia, para luego de su análisis establecer las conclusiones que se desprenden de la conjugación de la privacidad y administración de datos clínicos en sistemas informáticos.

Para atender estas cuestiones, será pertinente esbozar primero las líneas generales que imperan en la elaboración, el uso, almacenamiento y disposición final de la historia clínica, para luego indagar en el perfilamiento que ciertos cuerpos normativos en materia de protección de datos personales tienen en esta materia.

Así, por ejemplo, con la entrada en vigencia del Reglamento General de Protección de Datos (GDPR, por sus iniciales en inglés), surgen diferentes cuestiones que tanto profesionales sanitarios como pacientes deben atender para comprender la forma adecuada de generar una nueva cultura sobre el tratamiento de datos de carácter personal que reposan en las historias clínicas, siendo este, a su vez, un factor prevalente en la protección y la seguridad de la información de las personas físicas y un cambio igualmente importante dentro de las empresas del sector salud y las entidades sanitarias en lo que a su estructura jurídica, técnica y administrativa se refiere.

Sobre esto último, es importante tener en cuenta que los compendios normativos relativos a la protección de información personal afectan a todos los profesionales que operan en el sector sanitario, y su correcta aplicación puede llegar a presentar una mayor complejidad que otros controles profesionales, ya que el tipo de datos que ellos tratan son especialmente sensibles: los datos específicos relativos a la salud.

Para ahondar más en ello, debe tenerse como referente directo lo establecido en el artículo 5.º de la Ley 1581, en la cual se definen los datos sensibles como "aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como […] datos relativos a la salud". También es oportuno entender que, bajo los supuestos de operatividad adecuados, los datos consignados en las historias clínicas pueden ser tratados por diferentes perfiles y personas dentro de las instituciones que son responsables de su custodia, pero, alineados con la definición de datos semiprivados proporcionada por la ley[1], este tipo de información no podría encajar en esta última categoría por su innegable naturaleza íntima y reservada.

La información sobre las personas es una herramienta fundamental para la asistencia sanitaria. Tanto en el marco de la actividad sanitaria en el sector público como en el de la medicina privada, los pacientes proporcionan a los profesionales datos sobre su salud y colaboran en su obtención. Pero esto no significa que las personas renuncien a su intimidad ni a la confidencialidad de sus datos cuando reciben asistencia sanitaria. Por el contrario, los pacientes esperan que los profesionales que reciben dicha información respeten su deber de secreto y el carácter confidencial de los datos que manejan.

En este sentido, el Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías, en su Dictamen: Principios Éticos de la Sanidad en la Sociedad de

1 Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general. Ley 1266 de 2008.

la Información de 1999 señaló que "los datos de salud se refieren o afectan a la propia identidad y a ámbitos muy sensibles de la vida privada de los individuos"[2].

Esto se traduce en que los hospitales, clínicas privadas o públicas, centros sanitarios, médicos particulares, y especialmente en el contexto nacional, las entidades e instituciones prestadoras de servicios de salud (EPS e IPS, respectivamente) donde se tratan datos personales de categoría especial como los relativos a la salud de las personas deben velar por la protección de los derechos y los datos de los pacientes como núcleo fundamental básico de las relaciones médico-asistenciales.

No obstante, como es de entenderse, la salud es un elemento que se sustrae de su óptica eminentemente personalísima, y puede llegar a encuadrarse en una esfera mucho más amplia, que compacta tanto intereses colectivos como públicos, por lo que la información que se deriva de la actividad sanitaria puede llegar a ser abordada con fines diferentes de los que se circunscriben en estricto sentido a la autonomía de sus titulares, lo cual puede traducirse en justificar una excepción motivada a los derechos del paciente.

En este sentido, se toma como referencia lo establecido en la ley española de autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (Ley 41 de 2002), en que la confidencialidad y la intimidad relativa a la información relacionada con su salud pueden ser de gran interés para otros agentes cuyo objetivo esté determinado por la consecución de la salud pública como bien jurídico de fundamental relevancia para una sociedad democrática avanzada. La materialización de una ley cuyo enfoque sea el de la libertad, autonomía del paciente y su privacidad relacionada con los datos asociados a la prestación del servicio médico asistencial permite integrar adecuadamente nuevos modelos y herramientas cuyo enfoque sea el de hacer más eficiente y garantista la prestación de dicho servicio, para el caso la historia clínica electrónica interoperable.

En Colombia, en un sentido similar, el Decreto 2174 de 1996, mediante el cual se organizó el Sistema Obligatorio de Garantía de Calidad del Sistema General de Seguridad Social en Salud, en el numeral 4 de su artículo 5.° estableció como uno de los objetivos de la norma el estimular el desarrollo de un sistema de información que facilitara la realización de las labores de auditoría, vigilancia y control y contribuyera a una mayor información de los usuarios.

Junto con este decreto, el artículo 10 literal k de la Ley 1751 de 2015, por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones, se establece la intimidad como derecho, no solamente de los pacientes, sino de cualquier persona que pueda tener relación con la prestación del servicio de salud:

2 Ethical Principles of Health in the Information Society. Opinion of the European Group on Ethics in Science and New Technologies to the European Commission n.º 13. 30 de julio de 1999. Consultado en: https://op.europa.eu/en/publication-detail/-/publication/ea106948-e6f5-11e8-b690-01aa75ed71a1/language-en.

> Artículo 10. Derechos y deberes de las personas, relacionados con la prestación del servicio de salud. Las personas tienen los siguientes derechos relacionados con la prestación del servicio de salud: […] k) A la intimidad. Se garantiza *la confidencialidad* de toda la información que sea suministrada en el ámbito del acceso a los servicios de salud y de las condiciones de salud y enfermedad de la persona, sin perjuicio de la posibilidad, de acceso a la misma por los familiares en los eventos autorizados por la ley o las autoridades en las condiciones que esta determine.

Es pertinente destacar de esta línea regulatoria que la instrucción particular sobre la creación y disposición de la historia clínica, más allá de la finalidad prevista para ella, cual es la de facilitar la prestación de servicios médico-asistenciales, no se puede dejar de lado la íntima relación que su estructuración tiene con otros derechos y garantías que, como pacientes, son innegables y hacen parte de la esfera de protección que deben prever y proveer los prestadores de servicios de salud, tanto desde su papel administrativo como en el operativo.

Además, el artículo 19 de la Ley 1751 establece la necesidad de implementar un sistema único de información en salud, que integre los componentes demográficos, socioeconómicos, epidemiológicos, clínicos, administrativos y financieros de los actores del sistema de salud, en aras de garantizar un manejo veraz, oportuno, pertinente y transparente de los diferentes tipos de datos derivados de la prestación del servicio de salud[3].

De este modo, luego de varios años, con la expedición de la Ley 2015 de 2020 se da la primera repuesta en Colombia que atiende a la necesidad de crear dicho sistema único de información, diseñando para ello un esquema de interoperabilidad institucional en la que la manipulación y lectura de la historia clínica en formato electrónico es la base fundamental del sistema.

I. CONCEPTO Y NATURALEZA JURÍDICA DE LA HISTORIA CLÍNICA ELECTRÓNICA

La historia clínica se concibe como "el documento fundamental y elemental del saber médico, en donde se recoge la información confiada por el enfermo al médico para obtener el diagnóstico, el tratamiento y la posible curación de la enfermedad"[4].

En Colombia se han presentado diferentes acepciones que permiten entender la naturaleza de la historia clínica. Primeramente, la Ley 23 de 1981, sobre normas

3 Ley 1751 de 2015, artículo 19: Con el fin de alcanzar un manejo veraz, oportuno, pertinente y transparente de los diferentes tipos de datos generados por todos los actores, en sus diferentes niveles y su transformación en información para la toma de decisiones, se implementará una política que incluya un sistema único de información en salud, que integre los componentes demográficos, socioeconómicos, epidemiológicos, clínicos, administrativos y financieros. Los agentes del Sistema deben suministrar la información que requiera el Ministerio de Salud y Protección Social, en los términos y condiciones que se determine.

4 Laín, P. (1978). La historia clínica. En A. Balcells et al., Patología General. Tomo II. Fisiopatología y Propedéutica Clínica (pp. 1437-1487). Barcelona: Ed. Toray.

de ética médica, en su artículo 34 define la historia clínica como un "registro obligatorio de las condiciones de salud del paciente […] documento privado sometido a *reserva* que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley".

De forma concordante, la Resolución 1995 de 1999 del Ministerio de Salud, por la cual se establecen normas para el manejo de la historia clínica, la define como "un documento privado, obligatorio y sometido a *reserva*, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley" y como "el expediente conformado por el conjunto de documentos en los que se efectúa el registro obligatorio del estado de salud, los actos médicos y demás procedimientos ejecutados por el equipo de salud que interviene en la atención de un paciente, el cual también tiene el carácter de *reservado*" (artículo 1.º, literales a y d respectivamente).

Por su parte, la historia clínica electrónica, también conocida como digital o informatizada, es definida por el Grupo de Trabajo del artículo 29 de la Directiva 95/46[5] como "un historial médico completo o una documentación similar del estado de salud física y mental pasado y presente de un individuo, en formato electrónico, que permita acceder fácilmente a estos datos a efectos de tratamientos médicos y otros fines estrechamente relacionados".

Esta acepción permite entender la historia clínica electrónica como un historial único y trasversal a todos los prestadores de servicios de salud, donde se recaban los datos clínicos de los pacientes a partir de diversas fuentes y en distintos momentos, garantizando la disponibilidad de dicha información en formato electrónico, para todos los profesionales sanitarios e instituciones autorizados.

Junto con la integridad y disponibilidad de la información clínica se incluyen en estos sistemas diferentes funcionalidades adicionales que, entre otras cosas, permiten un mejor diagnóstico al poder comparar patologías y tratamientos, una mayor legibilidad de los datos en cuanto a la seguridad clínica asociada a errores por malas interpretaciones de los antecedentes médicos y una mayor eficacia en el ingreso y salida de documentos, entre los que se encuentran informes y fórmulas.

Desde Europa[6], pionera en esta materia, se ha determinado la importancia que para la atención sanitaria tienen los servicios electrónicos, técnicos e interoperables entre sí, siendo la herramienta por excelencia para *conseguir mejoras sustanciales de la*

5 Grupo de Trabajo sobre protección de datos del artículo 29. Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME). 00323/07/ES WP 131. Adoptado el 15 de febrero de 2007. Visto en https://www.apda.ad/sites/default/files/2018-10/wp131_es.pdf.

6 Comunicación de la Comisión Europea de Medio Ambiente, Salud Pública y Seguridad Alimentaria La salud electrónica – hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica abril de 2004, COM(2004)0356.

productividad como el instrumento del mañana para unos sistemas de salud centrados en el ciudadano y reestructurados, que al mismo tiempo respeten las distintas tradiciones multiculturales y plurilingües de Europa en el ámbito de la asistencia sanitaria[7].

II. DATOS CLÍNICOS COMO DATOS SENSIBLES

Por estas definiciones, se entiende que lo que es ponderable y transversal a ellas es el elemento restrictivo o reservado que se liga a la información que está consignada en las historias clínicas. La *reserva* a la que se hace referencia fue desarrollada ampliamente por la sentencia de la Corte Constitucional colombiana T-487/07[8], que a su vez reproduce lo establecido en años anteriores por la misma corporación en la sentencia T-729/02[9]. En estas sentencias se designa la información reservada, como un símil a los datos sensibles, ya que estos versan igualmente sobre información personal estrechamente relacionadas con los derechos fundamentales del titular de ella, a tal punto que se encuentra circunspecta a su órbita exclusiva y *no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones*[10].

El artículo 5.° de la Ley 1581 de 2012 (Ley Estatutaria de Protección de Datos Personales – [LEPDP]), define los datos sensibles como aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación. Además, la norma en mención proporciona una lista no taxativa de algunos datos personales que revisten la característica de ser sensibles, colocando dentro de ellos los datos relativos a la salud, a la vida sexual y los datos biométricos de las personas, no dejando duda de que información referente a los antecedentes neonatales, obstétricos o quirúrgicos del paciente, sus hábitos de vida, adicciones, consumo de tóxicos, alergias, enfermedades, antecedentes sociales y profesionales y cualquier otro dato personal relacionado con la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, así como las características genéticas heredadas y el análisis de muestras biológicas, incluidos todos ellos en la historia clínica tradicional, son sensibles y revisten el carácter de reservados, pues orbitan de forma exclusiva, en principio, a la esfera privada e íntima del individuo.

Por esta razón es que no solamente en Colombia sino en otros ordenamientos, sirviendo de ejemplo el GDPR en el marco de la Unión Europea, el tratamiento de estos datos se encuentra prohibido como primera medida, y solo habilitado en casos excepcionales. Así, la LEPDP y el GDPR establecen dichas excepciones de la siguiente manera:

7 Ibídem.
8 Corte Constitucional colombiana, sentencia T-487/07. M. P. Alberto Rojas Ríos.
9 Corte Constitucional colombiana, sentencia T-729/02. M. P. Eduardo Montealegre Lynett.
10 Ibídem.

Artículo 6.º de la LEPDP
a. El titular haya dado su autorización explícita a dicho tratamiento. b. El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. c. El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro. d. El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial e. El tratamiento tenga una finalidad histórica, estadística o científica.
Artículo 9.º del GDPR
a. El interesado ha dado su consentimiento explícito para el procesamiento de esos datos personales. b. El procesamiento es necesario para cumplir las obligaciones y ejercer los derechos específicos del responsable del tratamiento o del interesado en el ámbito del empleo y la seguridad social. c. El procesamiento es necesario para proteger los intereses vitales del interesado o de otra persona física donde el interesado es física o legalmente incapaz de dar su consentimiento. d. El procesamiento se lleva a cabo en el curso de sus actividades legítimas con las garantías adecuadas de una fundación, asociación o cualquier otro organismo sin fines de lucro. e. El procesamiento se refiere a los datos personales que el interesado hace públicamente manifiestamente; f. El procesamiento es necesario para el establecimiento, ejercicio o defensa de reclamos legales o cuando los tribunales están actuando en su capacidad judicial; g. El procesamiento es necesario por razones de interés público sustancial. h. El procesamiento es necesario para fines de medicina preventiva u ocupacional, para la evaluación de la capacidad de trabajo del empleado, el diagnóstico médico, la provisión de atención o tratamiento de salud o social o la gestión de sistemas y servicios de salud o asistencia social de conformidad con el contrato con un profesional de la salud. i. El procesamiento es necesario por razones de interés público en el área de la salud pública, como la protección contra amenazas transfronterizas graves para la salud o garantizar altos estándares de calidad y seguridad de la atención médica y de los medicamentos o dispositivos médicos. j. El procesamiento es necesario para fines de archivo en interés público, fines de investigación científica o histórica o fines estadístico.

De esta comparativa se sustraen ciertas ideas y consideraciones adicionales en materia de historias clínicas y tratamiento de datos de salud:

1. La autorización que proporcione el titular de la información (paciente) implica un consentimiento explícito y ajustado a necesidades y finalidades específicas relativas a la atención brindada por los profesionales de la salud. El responsable del tratamiento deberá estar en condiciones de probar en todos los casos no solamente que ha obtenido el consentimiento u autorización explícita de cada paciente, sino que este consentimiento explícito se dio basándose en información suficientemente exacta.

Este consentimiento se debe tener por diferenciado del consentimiento informado regulado en Colombia por los artículos 161, 182, 193 y 204 de la Constitución Política y los artículos 14, 15 y 18 de la Ley 23 de 1981 sobre el consentimiento, que se debe dar en la relación médico-pacientes para realizar los diferentes tratamientos médico-quirúrgicos que se prestan en torno a ella.

2. En Colombia, desde la LEPDP y en el contexto de la prestación de servicios de salud, no existe ninguna alternativa legal para realizar el tratamiento de datos personales del paciente sin que este proporcione su autorización, salvo que se

tenga la finalidad de salvaguardar su salud o su vida, y este se encuentre física o jurídicamente incapacitado, caso en el cual deberán ser sus representantes legales quienes proporcionen su autorización[11].

De modo general, el artículo 10 de la LEPDP, dentro los casos en los que no se requiere autorización del titular para el tratamiento de sus datos, contempla la urgencia médica o sanitaria como justificante para ello, lo cual implica que solo en los casos en que, por la especial y concreta situación de urgencia que imposibilite la obtención de la autorización del titular o lo particularmente problemático que resulte gestionarla por el apremio de la prestación del servicio médico, el riesgo o peligro para otros derechos fundamentales, tanto del paciente como de terceras personas, se podría llegar a prescindir de la autorización. No obstante, es de entenderse que en la medida en que esta situación crítica y manifiestamente urgente sea superada, el paciente deberá ser plenamente informado de los tratamientos y finalidades de los que fue objeto su información, a efectos de que este pueda validarlos y legitimarlos o, por el contrario, pueda decidir y exigir, como titular de los datos, su eliminación o supresión de las bases de datos de la entidad prestadora del servicio de salud o su oposición frente a tratamientos de datos futuros[12].

Esto quiere decir en últimas que, teóricamente, solo con la autorización del paciente o de sus representantes legales o en situaciones concretas de urgencia o riesgo para él o terceras personas se podría realizar legalmente un tratamiento de sus datos personales.

3. En principio, la previsión que se hace en el literal a del artículo 6.º del LEPDP relativa a la posibilidad de omitir la autorización del titular para tratar los datos sensibles en los casos que por ley no se requiera el otorgamiento de dicha autorización tiene cabida de forma limitada en materia de creación, alimentación y consulta de la historia clínica, ya que, salvo por la excepción consagrada en el artículo 10 del LEPDP (urgencia médica o sanitaria) y un concreto caso, no existe actualmente ningún mandato legal expreso en este sentido; y aun cuando existiera, tal como lo reconoció la Corte Constitucional colombiana en la sentencia C-748-11, de 6 de

11 En relación con el principio de finalidad, es de tenerse en cuenta que el tratamiento debe tener un propósito específico y explícito que sea acorde a la Constitución y la ley, de lo cual debe ser informado el titular de manera previa, clara, suficiente y que solo puede darse por un periodo, el cual no debe exceder del necesario para dar cumplimiento a la finalidad con la que estos fueron recaudados, teniendo en cuenta que los datos recaudados tengan una directa relación con el objetivo de la base de datos que los contiene. La utilización de los datos para una finalidad distinta a la consentida por el titular o la permitida por la ley de los datos personales deberá contar con autorización expresa para el nuevo tratamiento, esto es, para la recolección, el uso, el almacenamiento, la circulación o la supresión de estos. En este sentido puede verse el concepto de la Superintendencia de Industria y Comercio n.º 16-459471 del 27 de enero de 2017.

12 El derecho de oposición se refiere al derecho del titular de los datos a que no se lleve a cabo un determinado tratamiento de los mismos cuando haya motivos fundados y legítimos relacionados con alguna situación personal. El derecho de supresión, por su parte, faculta al titular de los datos para solicitar la eliminación de sus datos no guardan relación con la finalidad para la que se recogieron en su momento.

octubre de 2011[13], además de la necesidad de estar contenida en una ley, debería ajustarse a las garantías que otorga el *habeas data*, en relación con el principio de finalidad, cumpliendo con las exigencias del principio de proporcionalidad.

El caso concreto comentado es el que se establece en el Decreto Único Reglamentario del Sector Trabajo, 1072 de 2015, artículo 2.2.4.6.13 y las resoluciones 2346 de 2007 y 1918 de 2009 del Ministerio de Protección Social, artículos 16 y 17 respectivamente, de cuyo análisis se desprende que el médico laboral puede acceder a la historia clínica ocupacional, sin autorización del titular, realizando con ello tratamiento de datos sensibles de los pacientes, siempre que se cumplan tres requisitos fundamentales: (1) el responsable se encuentre actuando en calidad de empleador; (2) la ley le impone una obligación de efectuar investigación de incidentes, accidentes de trabajo y enfermedades laborales, para lo cual el médico laboral requiere conocer la historia clínica ocupacional del trabajador; y (3) la información sensible es únicamente de sus trabajadores[14].

4. A diferencia de la LEPDP, el GDPR establece otros mecanismos de legitimación del tratamiento de datos de salud que se sustraen de la autorización que en principio deben entregar el paciente o sus representantes legales y que no necesariamente deben validar previamente una urgencia médica o sanitaria para ello. Dichas previsiones se hacen con fines de (a) salud particular, como cuando los fines perseguidos se circunscriben a la medicina ocupacional o para evaluar la capacidad de trabajo del empleado, el diagnóstico médico: o (b) salud pública, como cuando se pretende prevenir pandemias o epidemias o cuando se busca validar la provisión de atención o tratamiento de salud y la gestión de los servicios de atención de la salud del sistema, para garantizar la calidad y la rentabilidad de los procedimientos utilizados e incluso para atender a las reclamaciones de beneficios y servicios en esquema nacional del servicio de salud.

La forma en que estos planteamientos se acogen permite entender cómo en regímenes de protección de datos personales con más experiencia, como lo es el del GDPR, atendiendo a unas finalidades excepcionales y taxativas, se puede dar cabida a una mayor injerencia de la autonomía de los responsables y encargados que realizan el tratamiento, llegando incluso a dejar de lado la misma autonomía del titular/paciente, en cuanto al derecho que le corresponde de decidir sobre el tratamiento de su información personal. En este sentido, tal y como señala el artículo 19 del Real Decreto 1718/2010[15] español, no es necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, de conformidad con lo dispuesto en el artículo 9.2h del GDPR,

13 Corte Constitucional colombiana, sentencia C-748-11 de 6 de octubre de 2011, M. P. Jorge Ignacio Pretelt.

14 Superintendencia de Industria y Comercio. Resolución 27116 de 2019.

15 Real Decreto 1718/2010, del 17 de diciembre, sobre receta médica y órdenes de dispensación. Visto en https://www.boe.es/buscar/pdf/2011/BOE-A-2011-1013-consolidado.pdf.

el cual dispone que no se requiere el consentimiento cuando el tratamiento es necesario para fines de prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social[16].

Esto lleva además a que se plantee la dificultad que tienen los agentes involucrados en la elaboración de la historia clínica para determinar, a ciencia cierta, quién es el titular de ella.

III. TITULARIDAD DE LA HISTORIA CLÍNICA

Debe tenerse en cuenta, como primera medida, que el tratamiento se da sobre datos personales relativos a la salud de los pacientes, independientemente de su fuente, por ejemplo, un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica *in vitro*, lo cual lleva a concluir que éste es el titular de información en ella consignada, lo que deriva en el entendimiento de que, frente a estos datos, le corresponden todos los derechos y prerrogativas consagrados en la LEPDP y demás normas concordantes y vigentes.

Concretamente respecto a la titularidad de la historia clínica electrónica interoperable, el artículo 6.º de la Ley 2015 de 2020[17] establece que la titularidad de ella está en cabeza del paciente, razón por la cual solo bajo la expresa y previa autorización de este los prestadores de servicios de salud, instituciones prestadoras de servicios de salud, profesionales independientes de la salud, servicios de transporte especial de pacientes y entidades con objeto social diferente pero que prestan servicios de salud[18] podrán tener acceso a ella.

Esto se corresponde con los principios de libertad y finalidad previstos en el artículo 4.º de la LEPDP, los cuales buscan reforzar las condiciones en las que el titular de los datos personales puede ejercer dominio sobre ellos, al punto de decidir quiénes pueden tener acceso a su información personal y quiénes no, o para cuáles finalidades sí y para cuáles no podrá ir destinada su información.

Lo anterior adquiere mucha importancia en términos de calidad del servicio. En un estudio presentado en 2019 en la *Revista Internacional de Informática Medica*[19],

16 Ibídem. No será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, de conformidad con lo dispuesto en los artículos 7, apartados 3 y 6; 8; y 11, apartado 2.a, de la Ley Orgánica 15/1999, del 13 de diciembre, de protección de datos de carácter personal. Las citadas actuaciones deberán tener por finalidad facilitar la asistencia médica y farmacéutica al paciente y permitir el control de la prestación farmacéutica del Sistema Nacional de Salud, incluidos los distintos regímenes especiales de las mutualidades de funcionarios.

17 Artículo 6.º. Titularidad. Cada persona será titular de su historia clínica electrónica, a la cual tendrán acceso, además del titular, los sujetos obligados en el artículo tercero de la presente ley, con el previo y expreso consentimiento de la persona o paciente de acuerdo con la normatividad vigente.

18 Ministerio de Salud de Colombia. Consulta hecha el 6 de febrero de 2020. Visto en https://www.minsalud.gov.co/Lists/FAQ/DispForm.aspx?ID=950&ContentTypeId=0x01003F0A1BD895162D4599DC199234219AC7.

19 AYAAD, O., ALLOUBANI, A., y otros, The role of electronic medical records in impro-

relativo al papel de los registros médicos electrónicos en relación con la calidad de los servicios de atención médica, tras una evaluación comparativa entre varios centros de salud se demostró que respecto de la posibilidad que tiene un sistema de historia clínica electrónica interoperable de proveer acceso interpretativo, "abierto" y de uso multiprofesional, en el sentido de que no solamente prestadores de servicio de salud sino, concretamente, médicos, enfermeros, personal asistencial y administrativo pueden acceder e incluso manipular la información consignada en la historia clínica electrónica interoperable, la existencia de la autorización o el consentimiento que dé el paciente sobre el tratamiento de su información personal en esos registros médicos electrónicos es determinante para la estimación positiva respecto de la calidad y eficiencia del servicio médico.

Entre otras cuestiones, la titularidad de la historia clínica electrónica interoperable deriva en otros asuntos de suma relevancia como el acceso a la información médico-asistencial y la trasmisión y transferencia de datos en ella contenida.

IV. USO DE LA HISTORIA CLÍNICA POR EL PERSONAL DE LOS CENTROS HOSPITALARIOS

La Ley 2015 de 2020 manifestó en su artículo 7.º, en el mismo sentido de su artículo precedente, que solo la persona titular de la historia clínica electrónica podrá autorizar el uso por terceros de la información total o parcial en ella contenida, de acuerdo con la normatividad vigente, lo cual, sin pretender encasillarse en lo que tiene que ver con su autorización, vale para mencionar que bajo los supuestos previamente analizados en los que el prestador del servicio de salud puede realizar el tratamiento de información personal del paciente[20], este goza de una legitimación derivada para que los funcionarios que coadyuvan en la labor de prestar el servicio de salud y que tengan participación en el flujo de información de los pacientes lo puedan hacer sin mayores restricciones.

No obstante, habría que considerar que de las competencias que cada usuario de la historia clínica electrónica interoperable tenga dentro del centro o institución de salud, bajo una arista del principio de proporcionalidad, dependerán las injerencias que ellos tengan respecto de la información personal que consultan. Así, una persona cuyas actividades se circunscriben exclusivamente a temas administrativos, respecto de los cuales la información consignada en la historia clínica, como el médico especialista, medicamentos y datos de contacto del paciente, no tendría por qué tener contacto con otro tipo de información mucho más sensible, respecto a la cual, por su carácter confidencial, en principio solo debe ser conocido por los médicos y personal asistencial tratantes.

ving the quality of health care services: Comparative study, International Journal of Medical Informatics, volume 127, 2019, págs. 63-67.

20 Estos son la autorización del paciente o de sus representantes legales o en situaciones concretas de urgencia o riesgo para el o terceras personas.

Gracias a la historia clínica electrónica interoperable, no solamente es posible imponer en el sistema de consulta este tipo de restricciones en cuanto a la información a la que cada usuario puede acceder, sino que además se puede lograr con ella una mejor identificación y gestión de los perfiles de acceso, de forma que solo aquellos profesionales autorizados podrán acceder a través de identificación con *login* o firma electrónica e incluso conocer quién accedió al sistema y qué contenidos fueron visualizados o modificados, con la fecha y la hora exacta.

En este sentido, se recuerda el caso del Tribunal Superior de Justicia de Navarra del 8 de febrero del 2012[21] en el que se determina la responsabilidad patrimonial del centro de salud responsable de la información del paciente, debido a que se logró comprobar más de 2800 accesos a la historia clínica electrónica por parte de 417 usuarios, que representaban 55 servicios diferentes entre hospitales, centros de salud, servicios ambulatorios y de transporte, siendo que el paciente en realidad solo había estado en un único hospital y había tomado apenas cuatro servicios médico-asistenciales.

En apoyo a lo anterior, se exalta lo establecido en la Resolución 1995 de 1999 del Ministerio de Salud, la cual en su artículo 14 señala que

> Podrán acceder a la información contenida en la historia clínica, en los términos previstos en la Ley: (1) El usuario. (2) El equipo de salud. (3) Las autoridades judiciales y de salud en los casos previstos en la ley. (4) Las demás personas determinadas en la ley. Parágrafo. El acceso a la historia clínica se entiende en todos los casos única y exclusivamente para los fines que de acuerdo con la ley resulten procedentes, debiendo en todo caso, mantenerse la reserva legal.

También se debe tener presente que el contexto de la historia clínica electrónica puede llevar a que se realice un tratamiento automático de la información y de los datos en ellos consignados, lo cual permite crear modelos eficientes e integrados que generen la información requerida de manera directa, evitar procesos manuales y proporcionar, entre otras cosas, mejores respaldos de los documentos clínicos generados en medio de la prestación del servicio de salud. No obstante, deviene una compleja situación que se puede llegar a presentar en el tratamiento de estos datos sensibles frente a su tratamiento automatizado, ya que al no existir un filtro humano, cuando menos residual, se deja de lado un control sobre los elementos que distinguen esta categoría de datos de alguna otra rúbrica separada. La "inteligencia artificial", sistema experto o algoritmo que se emplee para el procesamiento automático de los datos de los pacientes no tiene el desarrollo discrecional para frenar la actividad negativa que se puede dar en torno a esta importante y delicada información, como lo puede tener quien evalúa la situación (titular, encargado, responsable o usuario del dato) gracias a su percepción subjetiva.

21 Tribunal Superior de Justicia de Navarra, sentencia 111 del 8 de febrero del 2012. M. P. Antonio Rubio Pérez. Visto en: https://delajusticia.com/wp-content/uploads/2012/03/stsjnavarra.pdf.

V. TRANSFERENCIA Y TRANSMISIÓN DE DATOS DE LA HISTORIA CLÍNICA

La premisa de la Ley 2015 de 2020 es diseñar un esquema de interoperativilidad dentro del Sistema General de Seguridad Social en Salud, cuya base se encuentra en los recursos tecnológicos, en relación con las historias clínicas, como principal insumo de información para la adecuada prestación de los servicios médico-asistenciales; por tal motivo, en este acápite es indispensable tener claridad acerca de la definición de *interoperabilidad*.

Por *interoperabilidad* se entiende la capacidad de los sistemas de información y de los procedimientos a los que estos dan soporte de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos[22]. Esto puede lograrse con diferentes herramientas y tecnologías como lo son *blockchain* o *big data*, lo cual representa a su vez un análisis más minucioso de sus ventajas y desventajas[23].

En el mismo sentido se dan las consideraciones del Real Decreto 4/2010, del 8 de enero, por medio del cual se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica española[24]:

> La interoperabilidad es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Resulta necesaria para la cooperación, el desarrollo, la integración y la prestación de servicios conjuntos por las Administraciones públicas; para la ejecución de las diversas políticas públicas; para la realización de diferentes principios y derechos; para la transferencia de tecnología y la reutilización de aplicaciones en beneficio de una mejor eficiencia; para la cooperación entre diferentes aplicaciones que habiliten nuevos servicios; todo ello facilitando el desarrollo de la administración electrónica y de la sociedad de la información.

En el plano de la prestación del servicio de salud, la interoperabilidad debe ser evaluada como un todo, en el que sus dimensiones organizativas, semántica y técnica, permitir que los diferentes agentes que integran el Sistema General de Seguridad Social en Salud colombiano se integren de manera adecuada con el fin de obtener ventajas para los usuarios y para ellos mismos, derivadas de la escalada de información, de la aplicación de las arquitecturas modulares y multiplataforma, así como del compartir, de reutilizar y de colaborar entre sí[25]. Esto es consecuente con lo señalado por la Comisión Europea en 2012 en su *Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI*: "La interoperabilidad de

22 Ministerio Hacienda y AA. PP. 2018, Código de interoperabilidad: recopilación normativa. Primera edición 2017.

23 En este sentido, se recomienda la lectura de Escobar Borja, M. y Mercado Pérez, M. (2019). Big data: un análisis documental de su uso y aplicación en el contexto de la era digital. Revista La Propiedad Inmaterial. 28 (dic. 2019), 273-293.

24 Real Decreto 4/2010, del 8 de enero de 2010. Visto en: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1331.

25 Ibídem, artículo 7.

las soluciones de las TIC y del intercambio de datos es un requisito para una mejor coordinación e integración en toda la cadena de la prestación de atención sanitaria e intercambio de datos sanitarios, al tiempo que se impulsa el mercado único de la salud electrónica".

En este sentido, es posible estimar que aun cuando se haga uso de este sistema de interoperabilidad, el cual es visto jurídicamente como un todo, los prestadores de servicios de salud que tienen el contacto inicial con el paciente y crean y manipulan su historia clínica electrónica en un primer momento, conservan el papel de responsables del tratamiento y que frente a este sistema y el uso de la historia clínica electrónica interoperable, terceras personas que acceden a la información en ella almacenada asumen el papel tanto de encargados como de responsables derivados del primer prestador de servicios de salud, dependiendo de si existe una trasferencia o un transmisión de datos personales.

Esto significa, indiscutiblemente, que el sistema de interoperabilidad del que hace parte la historia clínica electrónica interoperable no fractura la relación hipotética que hay entre titular/paciente, responsable/prestadores de servicios de salud y encargados/terceros, salvo que así lo quiera directamente el paciente titular del dato, ya que, bajo la premisa de un mismo "servicio de salud", trasversal a todo el sistema y gracias a la libertad que tiene la persona de escoger entre las diferentes empresas prestadoras de servicios de salud o médicos particulares, aun cuando la información sea inequívoca para todos aquellos quienes tienen acceso a ella gracias a la historia clínica electrónica interoperable, será quien capture la información en cada momento o quien la utilice con cada consulta diferente del paciente quien deba asumir todas las obligaciones que corresponden al "responsable" en los términos de la LEPDP. Los encargados serán entonces todos aquellos terceros, diferentes al responsable, que ejecuten las órdenes del responsable y realicen el tratamiento de datos personales por cuenta de aquel. Esto llevaría a que se aplicaran, sin excepción, las normas relativas a las una trasferencias y transmisiones de datos personales, según el caso, especialmente las contenidas en el capítulo V del Decreto 1377 del 2013, hoy incorporado en el Decreto Único Reglamentario 1074 de 2015[26].

En cualquier caso, el artículo 12 de la misma Ley 2015 de 2020 establece la prohibición de divulgar los datos de cualquier persona consignados en la historia clínica electrónica interoperable por parte de quien hubiere tenido acceso a esta

26 Es oportuno hacer énfasis en lo señalado por la Corte Constitucional en la sentencia C-748 de 2011, en la cual se señala que "el encargado del tratamiento no puede ser el mismo responsable, pues se requiere que existan dos personas identificables e independientes, natural y jurídicamente, entre las cuales una –el responsable– le señala a la otra –el encargado– como quiere el procesamiento de unos determinados datos. En este orden, el encargado recibe unas instrucciones sobre la forma como los datos serán administrados. Volvamos al ejemplo de la historia clínica, en el que la institución de salud contrata con una compañía el procesamiento de las historias para que con un programa especial que puede determinar el responsable o la empresa contratada le organice la información contenida en ellas, siguiendo las indicaciones que establece el hospital. En este caso, el encargado del tratamiento de los datos es la persona jurídica que se contrata para el procesamiento de las hojas de vida".

información, a menos que cuente con la autorización del paciente o su representante legal, o se trate de situaciones de urgencia o riesgo inminente para la vida del paciente o terceros.

VI. CUSTODIA Y SEGURIDAD DE LAS HISTORIAS CLÍNICAS

Mediante la Resolución 1995 de 1999[27] del Ministerio de Salud se establece la obligación que tienen los prestadores de servicios de salud, de utilizar medios físicos o técnicos como computadoras y medios magneto-ópticos, cuando así lo consideren conveniente. Junto con esta previsión legal, se establece que aquellos programas automatizados que se diseñen y utilicen para el manejo de las historias clínicas, junto con los equipos donde esta esté soportada, deberán estar provistos de mecanismos de seguridad que imposibiliten la incorporación de modificaciones a la historia clínica una vez se registren y guarden los datos.

Junto con esta medida de seguridad, el Ministerio de la época continúa con su discurso de avanzada, al obligar a los prestadores de servicios de salud a proteger la reserva de la historia clínica mediante mecanismos que impidan el acceso de personal no autorizado para conocerla y adoptar las medidas tendientes a evitar la destrucción de los registros en forma accidental o provocada.

Además, ya para la época quienes administraban las historias clínicas de los pacientes debían permitir la identificación del personal responsable de los datos consignados, mediante códigos, indicadores u otros medios que reemplacen la firma y el sello de las historias en medios físicos, para con ello establecer con exactitud quién realizó los registros, así como la hora y fecha del registro.

En cuanto a la conservación general de las historias clínicas, el artículo 25 de la Ley 594 de 2000 plantea la imperiosa necesidad de implementar para este tipo de registros reglamentación específica relacionada con los tiempos de retención documental. Dicha observación fue en la Resolución 839 de 2017[28], en cuyo artículo 3.º se establece que la historia clínica debe retenerse y conservarse por el responsable de su custodia, por un periodo general mínimo de quince años y uno especial de treinta para las historias clínicas de víctimas de violaciones de derechos humanos o infracciones graves al derecho internacional humanitario, contados en ambos casos a partir de la fecha de la última atención.

Para ello se diseñan dos diferentes niveles, que pretenden garantizar la forma en la que, de forma estructurada, se debe garantizar el archivo y consulta de la información médica de los pacientes. De esta forma, durante los cinco primeros años dicha retención y conservación se hará en el archivo de gestión y los diez años siguientes en el archivo central. En proporción, para las historias clínicas de víctimas de violaciones de derechos humanos o infracciones graves al derecho

27 Ministerio de Salud, Resolución 1995 del 8 de julio de 1999, artículo 18.
28 Ministerio de Salud y Protección Social, Resolución 839 del 23 de marzo de 2017.

internacional humanitario los tiempos de custodia en estos niveles serán de diez y veinte años, respectivamente.

Para salvaguardar el interés que pueda tener el paciente, titular de dicha historia clínica, una vez cumplidos los tiempos de custodia se debe garantizar la entrega directa de esta a su titular, para lo cual se dispone la publicación de mínimo dos avisos en un diario de amplia circulación nacional, con un intervalo de ocho días entre el primer aviso y el segundo, en los que indicará el plazo y las condiciones para la citada entrega, plazo que podrá extenderse hasta por dos meses más, contados a partir de la publicación del último aviso.

Además, si al momento de tener en custodia una historia clínica esta se constituye como prueba dentro de un proceso relacionado con delitos de lesa humanidad, la conservación será permanente, lo cual deberá garantizar la entidad a cuyo cargo se encuentre la custodia, utilizando para tal fin los medios que considere necesarios.

Con ello se advierte cómo veinte años antes de las incorporaciones normativas de la Ley 2015 de 2020 ya existía una preocupación latente por salvaguardar la integridad de la información personal relacionada con la atención médica y los padecimientos físicos y psicológicos de las personas. Habría que plantearse si con los cambios técnicos que presenta la historia clínica electrónica interoperable los términos previamente relacionados tienen la misma vigencia o si, por el contrario, tendrán que ser modificados, habida cuenta de las ventajas que en términos de seguridad, disponibilidad e integridad plantea el sistema.

En este momento la ley colombiana en materia de historia clínica electrónica determina como medidas concretas de seguridad y custodia de información, adicionales a las ya mencionadas, las consignadas en su artículo 13:

> Los actores […] deberán establecer un plan de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, para lo cual establecerán una estrategia a través de la cual deberán realizar periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deberán contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo mediante la adopción de los lineamientos para la administración de la seguridad de la información y la seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones o quien haga sus veces.

Para dicha *evaluación de riesgo* vale la pena tener en cuenta las figuras que contempla el GDPR relativas a la evaluación de impacto que evalúe el origen, la naturaleza, la particularidad y la gravedad del riesgo asociado al tratamiento (artículo 35), el registro de actividades de tratamiento (artículo 30) y protección desde el diseño y por defecto (artículo 25).

En cuanto a las medidas de seguridad relacionadas en la Ley 1581 de 2012, el principio de seguridad establece que la información sujeta a tratamiento por el responsable del o encargado del tratamiento a que se refiere dicha ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

CONCLUSIONES

La historia clínica, como uno de los principales insumos con los que cuentan los profesionales de la salud para la prestación adecuada del servicio, está en condiciones de adecuar su presentación al uso de las nuevas tecnologías, aprovechando las ventajas que brindan los sistemas de información, entre estos, la confidencialidad e integridad de los datos contenidos en el historial médico-asistencial de los pacientes, no solo para conseguir una mayor eficacia sino también para preservar y garantizar derechos fundamentales de los titulares de los datos, tales como el derecho a la salud, el derecho a la intimidad y el *habeas data*.

La cuestión de fondo que plantea el uso de la historia clínica electrónica es la forma en que, habida cuenta de las ventajas que trae su implementación en un esquema de interoperabilidad institucional y profesional en materia de salud, los datos de los individuos que participan en este y, específicamente, de los pacientes, atiende a su autonomía y en atención al respeto que debe existir de forma permanente al principio de información en materia médica.

Estas precisiones se dan en función de una premisa fundamental y es la de que todos los individuos y todos los pacientes tienen derecho a la intimidad y pueden esperar de manera razonable que la confidencialidad y la protección de su información personal serán rigurosamente atendidos y protegidos por todos los profesionales sanitarios y por todas las demás personas con funciones incluso administrativas. Esta expectativa es también válida por lo que se refiere a los sistemas de historias médicas electrónicas.

En Colombia se cuenta con una serie de normas más o menos amplia que se encarga de regular la forma en que los registros médicos de los pacientes deben ser utilizados en función de la ponderación entre la eficacia del sistema de salud y la defensa del derecho de los ciudadanos. Estas normas, pese a tener una nada despreciable antigüedad, dilucidaban desde su expedición la necesidad de crear un esquema de funcionamiento trasversal a todos los prestadores de servicios de salud. En este sentido, la interoperabilidad en materia de salud busca integrar la forma en que los diferentes agentes del sistema participan en la creación de una historia clínica que sea única y dinámica, en el sentido de que, frente a nuevos cambios en el estado de salud de los pacientes, estos puedan ser incluidos en el registro electrónico, y pueda ser consultado de forma casi inmediata por todos aquellos que estén legitimados para ello.

Bajo esta clara noción, una pregunta que debe abordarse respecto a la manipulación del sistema que contiene la historia clínica electrónica es: ¿Quiénes pueden consultar la historia clínica del paciente y bajo qué condiciones pueden hacerlo? Esta cuestión tiene repercusión en el ámbito del *habeas data*, ya que si se considera la naturaleza de la información que está contenida en ella y se entiende la sensibilidad que atañe a ella, será fácil entender que las normas que conciernen a la protección de los datos personales tienen una aplicación directa en este sistema electrónico, bajo la premisa de que al titular de la información, como dueño de ella, le compete tomar las decisiones respecto a quienes y en qué forma se realizará su tratamiento.

La anterior ha derivado en que normas ya vigentes, como la Resolución 839 de 2017 y la Ley 2015 de 2020, especializadas en materia de historia clínica, aborden, cuando menos de forma superficial, el respeto en su aplicación, por el régimen vigente en Colombia, en materia de protección de datos personales. Así, el uso, manejo, recolección, tratamiento de la información y disposición final de las historias clínicas, tanto las contenidas en medios físicos como las electrónicas que hacen parte del sistema de interoperabilidad, deberá observar lo correspondiente a la protección de datos personales, de que tratan la Ley 1581 de 2012 (LEPDP), sus normas reglamentarias y las disposiciones que las modifiquen o sustituyan.

Es de esperar que ciertas cuestiones complejas deriven de esto último, ya que aun cuando las normas que se circunscriben a la implementación de la historia clínica electrónica en Colombia hacen una remisión integral a la LEPDP, los sujetos de la norma 2015 de 2020, es decir, los prestadores de servicios de salud, pueden tener problemas en llevar a la práctica algunos elementos de este par de normas, tales como las autorizaciones de acceso, modificación y supresión de la información, medidas adecuadas de seguridad y atención de derechos por parte de los titulares de la información.

En este sentido, es viable, cuando menos como base para fijar criterios interpretativos, poner en el mapa de análisis y estudio otros contextos jurídicos, como puede ser el de la Unión Europea, ya que, en aras de construir un sistema regional adecuado para todas las naciones que la integran, han adquirido una amplia experiencia en la expedición y ejecución de regulaciones cuyos objeto de aplicación son tanto la protección a la autonomía del paciente y su historia clínica como la salvaguarda de su información personal.

No obstante, dentro del estudio desarrollado para el presente escrito se tiene a modo de conclusión que una de las mayores preocupaciones que surgen en materia de historia clínica electrónica, cual es el consentimiento del paciente para el tratamiento de sus datos personales por parte de los prestadores de servicios de salud, podía ser resuelto directamente por la LEPDP: El tratamiento o, lo que es lo mismo, la inclusión de los datos relativos a la salud de las personas dentro del sistema de la historia clínica electrónica interoperable solo podrá darse (a) con la autorización del paciente o de sus representantes legales o (b) en situaciones concretas de urgencia o riesgo para él o para terceras personas.

En tal sentido, es adecuado afirmar que el bloque normativo conformado por las leyes que regulan la historia clínica tradicional, el régimen vigente en materia de protección de datos personales y la reciente Ley 2015 de 2020 constituye un adecuado listado de derechos y obligaciones en favor de los pacientes, que, bajo su lectura armónica junto con otras fuentes auxiliares como el RGPD[29], permite garantizar la adecuada protección de la privacidad de los titulares de estos datos personales, categorizados como sensibles.

REFERENCIAS

DOCTRINA

Ayaad, O., Alloubani, A., y otros (2019). The role of electronic medical records in improving the quality of health care services: Comparative study, International Journal of Medical Informatics, volume 127, págs. 63-67.

Calenti, R. (2013). Historia clínica electrónica: accesos compatibles. En J. Cantero y A. Palomar (dirs.), *Tratado de Derecho Sanitario* (vol. I). Cizur Menor: Ed. Aranzadi.

Criado, J. I. (2013). Interoperabilidad y política sanitaria en España. El caso de la Historia Clínica Digital desde una perspectiva intergubernamental. *Revista Castellano-Manchega de Ciencias Sociales*, 15, 73-94.

Comunicación de la Comisión Europea de Medio Ambiente, Salud Pública y Seguridad Alimentaria (2004) La salud electrónica, hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica abril de 2004, COM(2004) 0356.

Ethical Principles of Health in the Information Society (1999). Opinion of the European Group on Ethics in Science and New Technologies to the European Commission n.° 13, 30 de julio de 1999.

De Cossío, P. (2009). La confidencialidad de los datos médicos. En VV. AA., Derecho y medicina: cuestiones jurídicas para profesionales de la salud. Cizur Menor: Thomson Reuters Aranzadi.

Escobar Borja, M. y Mercado Pérez, M. (2019). Big data: un análisis documental de su uso y aplicación en el contexto de la era digital. Revista La Propiedad Inmaterial. 28 (dic. 2019), 273-293.

Fundación Telefónica. (2018) Sociedad Digital en España 2018. Editorial Taurus.

Grupo de Trabajo sobre protección de datos del artículo 29. Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales

29 Según el concepto de la SIC del 8 de junio de 2018, radicado n.º 18-154131, la autoridad de control colombiana es concluyente al establecer que el RGPD puede ser utilizado en nuestro ordenamiento como una fuente de interpretación auxiliar a la Ley 1581 de 2012.

médicos electrónicos (HME). 00323/07/ES WP 131. Adoptado el 15 de febrero de 2007.

LAÍN, P. (1978). La historia clínica. En A. Balcells et al., *Patología General. Tomo II. Fisiopatología y Propedéutica Clínica* (pp. 1437-1487). Barcelona: Ed. Toray.

LIU, J., LUO, L., ZHANG, R., & HUANG, T. (2013). Patient satisfaction with electronic medical/health record: A systematic review. Scandinavian Journal of Caring Sciences, 27(4), 785-791.

MARTÍNEZ DEVIA, A. 2019. La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? Revista La Propiedad Inmaterial. 27 (jun. 2019), 5-23.

MINISTERIO HACIENDA y AA. PP. (2018), Código de interoperabilidad: recopilación normativa. Primera edición 2017.

PELAYO, S. (2001). Aspectos jurídicos relacionados con la historia clínica. En L. Martínez-Calcerrada, *Derecho Médico: Tratado de Derecho Sanitario* (tomo I). Madrid: Colex.

RODRÍGUEZ, R. (2009). La información sanitaria y la historia clínica. En VV. AA., *Derecho y medicina: cuestiones jurídicas para profesionales de la salud*. Cizur Menor: Thomson Reuters Aranzadi.

SÁNCHEZ-CARO, J. (2010). El uso y acceso a la historia clínica electrónica y la protección de datos. En A. Troncoso (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*. Cizur Menor: Civitas y Thomson-Reuters.

NORMATIVIDAD

Ley 1581 de 2012. Colombia.

Ley 1751 de 2015. Colombia.

Ley 2015 de 2020. Colombia.

Ley 23 de 1981. Colombia.

Ley 41 de 2002. España.

Ministerio de Salud y Protección Social, Resolución 839 del 23 de marzo de 2017. Colombia.

Ministerio de Salud, Resolución 1995 del 8 de julio de 1999, artículo 18. Colombia.

Ministerio de Protección Social, Resolución 2346 de 2007, artículo 16. Colombia.

Ministerio de Protección Social, Resolución 1918 de 2009, artículo 17. Colombia.

Superintendencia de Industria y Comercio, Resolución 27116 de 2019. Colombia.

Real Decreto 1718/2010, del 17 de diciembre, sobre receta médica y órdenes de dispensación. España.

Real Decreto 4/2010, del 8 de enero de 2010. España.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. España.

JURISPRUDENCIA

Corte Constitucional colombiana, sentencia C-748-11 del 6 de octubre de 2011, M. P. Jorge Ignacio Pretelt.

Corte Constitucional colombiana, sentencia T-487/07 del 25 de junio de 2007, M. P. Alberto Rojas Ríos.

Corte Constitucional colombiana, sentencia T-729/02 del 5 de septiembre de 2002, M. P. Eduardo Montealegre Lynett.

Tribunal Superior de Justicia de Navarra, sentencia 111/2012 del 8 de febrero del 2012. M. P. Antonio Rubio Pérez.