Régimen de Protección de Datos: Un desafío Desde la Interoperabilidad de la Historia Clínica y la Ética Deontológica del Profesional en Salud.

Elizabeth Lalinde Vanegas[1]

Resumen

Este artículo plantea un estudio acerca de los aportes y desafíos que trae el Régimen de Protección de Datos para los profesionales de la salud, al momento de abordar la historia clínica desde una mirada ética y la interoperabilidad del documento clínico. Desarrollar esta propuesta investigativa ha de permitir fomentar en los profesionales de la salud una enseñanza- aprendizaje en un esfuerzo por equilibrar la disponibilidad de la información y la privacidad de los titulares, mediante un acceso regulado a los datos, respetando las normas de seguridad y privacidad impuestas para salvaguardar los intereses de los pacientes. Considerar esta teoría científica es imperativo para establecer relaciones éticas que contribuyan a una mejor comprensión de la Protección de los Datos en Colombia a través del Régimen de Protección de Datos, especialmente en un contexto de la privacidad y seguridad de la información. Lo anterior, teniendo en cuenta el actuar transparente del profesional en Salud que a todas luces respete la voluntad de las personas. Esto significa cumplir con las normativas y estándares éticos instaurados en relación con la protección de la información en Colombia, desde una mirada ética y el manejo de los datos personales desde el respeto por la autonomía, la privacidad, la

[1] Profesional en Desarrollo Familiar de la Universidad Católica Luis Amigó. Estudiante de Derecho de la Universidad Católica Luis Amigó. Correo electrónico elizabeth.lalindeva@amigo.edu.co. Este artículo es presentado para optar al título de abogada de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Luis Amigó. Tutor Dany Steven Gómez Agudelo.

confidencialidad, el cumplimiento de los modelos éticos y la responsabilidad demostrada en el tratamiento de la información personal.

***Palabras clave*: ética deontológica, interoperabilidad de la historia clínica, régimen de protección de datos, responsabilidad demostrada, principios orientadores del régimen de protección de datos.**

Summary

This article presents a study on the contributions and challenges that the Data Protection Regime brings to health professionals when approaching the medical history from an ethical perspective of health professionals and the interoperability of the clinical document. Developing this research proposal must allow health professionals to be taught and learned in an effort to balance the availability of information and the privacy of the holders, through regulated access to data, respecting the security and privacy standards imposed to safeguard the interests of patients. Building this scientific theory is imperative to establish ethical relationships that contribute to a better understanding of Data Protection in Colombia through the Data Protection Regime; especially in a context of privacy and information security. The foregoing, taking into account the transparent action of the health professional who clearly respects the will of the people. This means complying with the regulations and ethical standards established in relation to the protection of personal data in Colombia. From an ethical perspective, the handling of personal data emphasizes respect for autonomy and privacy, confidentiality, compliance with ethical models and demonstrated responsibility in the treatment of personal information.

Keywords: ethics of ethics, interoperability, data protection regime, demonstrated responsibility, guiding principles.

Sumario: introducción. **1.** Aportes Constitucionales, Normativos y Jurisprudenciales que sirven de orientación al Régimen de Protección de Datos en Colombia. **2.** Principios orientadores del Régimen de Protección de Datos. **3.** Discusión. **4.** Referencias.

Introducción

La protección de datos personales en Colombia procura proteger la privacidad de las personas y garantizar el uso responsable de la información desde una mirada ética. Supone un desafío para el profesional de la salud que interviene en el tratamiento del dato personal, quien en su quehacer profesional se encuentra enfrentado a una disyuntiva en relación con los aportes y desafíos que trae consigo la implementación del Régimen de Protección de Datos Personales al momento de abordar la historia clínica, el uso de los sistemas de información, y el secreto profesional.

Al respecto, López (2014), en su escrito Antecedentes Internacionales en Materia de Privacidad y Protección de Datos Personales, nos advierte acerca de la necesidad de "recopilar y registrar la información personal en computadoras, bancos de datos y otros dispositivos, tanto por las entidades públicas como las particulares o entidades privadas" (p.109), desde una legislación que garantice que la información relativa a la vida privada de las personas no sea utilizada por sujetos no autorizados, para fines no autorizados.

En este sentido, el derecho a la privacidad y la protección de los datos personales en Colombia plantea el reto de adoptar y mejorar un marco normativo amplio y suficiente que permita contrarrestar los peligros derivados de una carencia normativa y la ausencia de políticas

> públicas que incidan en las organizaciones, de modo que tal, que sus actores no se vean amenazados por la implementación de nuevos regímenes o nuevas tecnologías al momento de ejercer su labor y garantizar el derecho fundamental a la privacidad; sin pasar el límite de lo legal e incurrir en arbitrariedades.

Para garantizar este propósito vale la pena considerar entonces lo propuesto por Ramírez (2015), quien al referirse al derecho a la intimidad como un "derecho erga omnes, lo legitima para ser ejercido por cualquier persona en cuanto tiene una clara conexión con la dignidad humana y lo prevalece sobre el derecho a la información". (p.193).

No lejos de esta realidad, y tomando como referencia la intención de López (2014), aludiendo al Comité de los Derechos Humanos; este advierte la exigencia "en términos generales de adoptar medidas para que la información relativa a la vida privada de los individuos no esté disponible para personas no autorizadas para ello" (p.109).

Se trata pues, al llegar a este punto de vislumbrar que para satisfacer la aspiración de este trabajo investigativo, se debe comprender que el derecho a la privacidad por sí solo no garantiza la libertad y los derechos de las personas dentro de un medio de protección jurídica que preserve la seguridad de los datos, las medidas técnicas, organizativas y administrativas que garanticen el control de los profesionales de la salud de respetar los derechos de los titulares desde el secreto profesional al momento de elaborar informaciones referentes a seres identificados, evitando la manipulación, perdida o destrucción de la información sensible registrada en la historia clínica; para lo cual se hace necesario proponer la creación de políticas públicas y decretos reglamentarios, que en alianza con el sector

privado, permitan a los profesionales de la salud, gobernar los datos desde una responsabilidad demostrada.

Dicho esto, conviene recordar los derechos y deberes en el marco de la historia clínica, que nos evoca el "derecho constitucional, al deber de información y el secreto profesional, como obligaciones de mayor significado en el proceso de elaboración del documento medico clínico, en razón a los efectos que estos ocasionan en la autonomía e intimidad del paciente" (Blanco, 2019, p. 154).

Los aportes y desafíos que trae consigo el Régimen de Protección de Datos Personales en el siglo XXI, obliga a los Estados a crear políticas públicas que protejan al paciente en su máximo nivel de privacidad, en razón a la necesidad de garantizar el derecho constitucional a la intimidad y demás derechos conexos.

Abordar los aportes y desafíos que trae este régimen especial y la interoperabilidad de la historia clínica en el ejercicio de la labor del profesional en salud, implica hacer un ejercicio exploratorio profesional y responsable desde un análisis jurisprudencial, con el fin de comprender cómo la ausencia de proyectos relativos a la protección de los datos, afecta el tratamiento de la información por parte de los profesionales del sector sanitario al momento de abordar la historia clínica y prestar la atención en salud, así como autorregularse obligatoriamente por el Código deontológico, guardar y transmitir la información bajo las limitaciones propias que pueden enfrentar al momento de garantizar la protección integral y los principios rectores para el tratamiento de los datos.

El desarrollo de este artículo tuvo como propósito definir cuáles son los aportes y desafíos que el régimen de protección de datos presenta en el quehacer del profesional en salud y la

interoperabilidad al momento de garantizar los derechos de los titulares según el régimen de protección de datos y la normatividad vigente en Colombia 2020-2023.

Para el logro del fin propuesto, se formularon los siguientes objetivos específicos: 1). Definir los aportes y desafíos del Régimen de Protección de datos en los profesionales de Salud en Colombia 2020-2023. 2). Precisar los principios orientadores del Régimen de Protección de Datos para el quehacer del profesional en salud en Colombia 2020-2023. 3). Determinar los desafíos que presentan los profesionales del área de la salud al momento de garantizar la ética deontológica y el cumplimiento del Régimen de Protección de Datos Personales en su ejercicio profesional, según la normatividad vigente en Colombia 2020-2023.

Metodología

La propuesta metodológica para el desarrollo de este artículo se llevó a cabo desde una investigación socio-jurídica, la cual reveló cómo este régimen especializado de Protección de Datos reconoce y protege el derecho a la intimidad y a la protección de la información de los titulares en cumplimiento del mandato legal.

El método empleado fue cualitativo, el cual permitió crear conocimiento y obtener una profunda comprensión del fenómeno de estudio, centrar la recopilación de datos a través de métodos de recolección de información por diferentes fuentes documentales, como revistas científicas, que permitieron analizar las dimensiones de los datos personales, y de esta manera facilitar el acceso de información objetiva que responda a la pregunta objeto de investigación.

Así, las cosas, acoger este tipo de investigación facilitó mantener una postura neutral en la recolección de los datos y asumir una actitud exploratoria, comprender las opiniones y motivaciones de los diferentes autores, desarrollar ideas e hipótesis y utilizar técnicas no estructuradas.

La recolección de la información se dio a través de la técnica de Investigación documental, considerando la recopilación, selección de información, organización y análisis de cincuenta y tres fuentes documentales existentes para analizar los datos, y ofrecer resultados lógicos, soportados en la matriz de antecedentes como instrumento metodológico que posibilitó analizar y sistematizar la experiencia cumpliendo con los criterios de inclusión y exclusión tales como relevancia temática, tipo de documento, idioma y calidad metodológica. Así mismo, esta técnica de investigación permitió identificar adecuadamente el problema jurídico a estudiar, realizar un análisis interrelacionar del título de investigación y los objetivos propuestos para la investigación y revisar hipótesis, analizar categorías y contrastar con el estado del arte.

Esta investigación tuvo un enfoque crítico y reflexivo en relación a los temas propuestos desde la interdisciplinariedad, buscando comprender los fenómenos socio-jurídicos, con un énfasis en la argumentación que permitió construir razonamientos confiables y objetivos basados en el análisis de la incidencia de la ética deontológica, la interoperabilidad, el régimen de protección de datos, la responsabilidad demostrada y los principios orientadores de la protección de datos personales en el ejercicio del profesional en salud.

Paralelamente, desde la perspectiva teórica el trabajo investigativo se direccionó a través de la teoría fundamentada, buscando construir y edificar supuestos a partir de los datos

recopilados, en lugar de probar hipótesis preexistentes, permitiendo una teoría que emerja de manera inductiva.

Para una mejor comprensión de lo planteado en este artículo se definieron cuatro capítulos que interrelacionados entre sí dan cuenta de los aportes y desafíos que enfrentan los profesionales en salud, al momento de garantizar el cumplimiento del régimen de protección de datos personales y la tutela de los derechos de los titulares de la información.

Como resultado de estos capítulos se abarcan temas como el régimen de protección de datos personales que permite al lector ubicar su génesis en la historia, el desarrollo actual de la normatividad vigente en Colombia y el desafío que representa el sistema para los profesionales en salud, así mismo se planteó la exposición de los principios orientadores de protección de datos, con el fin de que el leyente logre una mejor comprensión de la parte estructural del sistema jurídico en tanto cumplen una función e integración del ordenamiento normativo, se aborda la ética deontológica desde la perspectiva del profesional en salud, y finalmente se precisó sobre la interoperabilidad desde el marco normativo de la historia clínica y su incidencia en la protección de datos personales en Colombia.

1. Aportes Constitucionales, Normativos y Jurisprudenciales que Sirven de Orientación al Régimen de Protección de Datos en Colombia.

El presente acápite tiene por objeto identificar los principales aportes constitucionales, normativos y jurisprudenciales que sirven de orientación al régimen de protección de datos en el ordenamiento jurídico colombiano.

En un primer momento es preciso recordar que la historia del régimen de protección de datos comienza con la Declaración Universal de los Derechos Humanos aprobada por la Asamblea General de las Naciones Unidas celebrada en Paris en 1948. Dicha declaración no se refiere directamente a la protección de los datos personales como un derecho fundamental, más bien, su interés declara el derecho de las personas de preservar su privacidad. El artículo 12, de dicha declaración dispone que: "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Resolución 217 A, 1948, Art. 12).

Ahora bien, en Colombia este mismo contexto histórico tiene su origen en la Constitución de 1991, cuando en su artículo 15, establece el deber legal de custodiar y proteger la intimidad personal y familiar de todas las personas, y en lógica con este precepto normativo, pretende el legislador de manera progresiva y conexa, regular aspectos relacionados con la protección de los datos personales, estableciendo la necesidad de clasificar los datos como aquella información asociada a una persona que permita su identificación, como lo es su documento de identidad, lugar de nacimiento, estado civil, trayectoria académica, entre otros.

Dicho esto, y como quiera que se hace necesario ahondar en el tema; es preciso realizar un análisis de su génesis como lo hemos planteado hasta aquí, al hacer un breve recuento del contexto histórico en esta materia, y más importante aún, es comprender cómo los avances normativos y tecnológicos han permitido regular en detalle aspectos relacionados con la privacidad de las personas a través del habeas data, los datos personales y la interoperabilidad.

En tal sentido es necesario precisar los aportes constitucionales, normativos y jurisprudenciales que sirven de orientación al régimen de protección de datos en Colombia, y reconocer la existencia de la relación íntima e inescindible que se presenta entre el derecho a la intimidad personal y familiar, y el régimen de protección de datos personales, como mecanismo que legitima los derechos y libertades de los individuos.

Seguidamente, se debe recordar que el régimen de protección de datos personales como sistema hibrido especializado que busca garantizar la legalidad de los titulares y el resguardo de los derechos fundamentales de todas las personas naturales, ha significado un desafío para los profesionales de la salud al momento de intervenir en el tratamiento del dato personal, abordar la historia clínica y garantizar la intimidad personal y familiar a través de sus metodologías internas.

De esta forma se manifiesta que la correcta administración de los datos personales representa para las organizaciones y los profesionales de la salud uno de los mayores retos de los últimos tiempos. La manera de acceder a los sistemas de información, el desafío de cumplir con los protocolos del régimen de protección de datos, y la alta responsabilidad de las entidades de garantizar los derechos a la vida privada de las personas, la intimidad y la protección de la información, así como el cumplimiento de los principios que rigen la protección de los datos personales, tales como: responsabilidad demostrada, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, los cuales en última instancia, buscan la satisfacción del marco normativo de protección de datos, la interoperabilidad de la historia clínica, y la ética deontológica del profesional en salud.

Por todo lo anterior, y al llegar a este punto, vale la pena considerar el aporte que nos hace Aguilar, al hacer referencia a la "globalización de las nuevas tecnologías", los datos personales, y su incidencia en el respaldo de la responsabilidad demostrada (2018, p.6).

> Admitamos que la incorporación de nuevos avances tecnológicos trae consigo una brecha digital que, de no ser atendida en debida forma, conlleva a unas consecuencias legales en materia de protección de datos personales; lo que supone un mayor esfuerzo de los operadores de salud, al momento de garantizar la responsabilidad demostrada, el respaldo y la efectiva protección de la información en el tratamiento de los datos personales.

Así las cosas, y para una mejor comprensión de lo propuesto en estas líneas, se toma como punto de partida, el desarrollo de los aportes constitucionales, normativos y jurisprudenciales existentes en Colombia, que, para el propósito de este artículo, permitirán tener una visión más amplia y dogmática de lo que propone este régimen especializado para la garantía de los derechos de los titulares de la información.

1.1 Aportes Constitucionales Sobre el Régimen de Protección de Datos en Colombia.

La protección de los datos personales en Colombia se fundamenta en la Constitución Política de 1991, quien en su artículo 15, versa:

> "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar". (Constitución Política de Colombia, 1991, Art 15).

Con esta argumentación pareciera ser que el legislador al momento de pensar en los derechos de los titulares de la información, estableció unas garantías Constitucionales que propenden fijar los límites propios para lograr el equilibrio entre la intimidad personal y familiar, y el deber del Estado de procurar en todo momento que en el tratamiento del dato personal, no se vulneren las libertades de las personas, especialmente en lo que tiene que ver con la información privada y sensible, categorizada como inviolable, como lo es para el particular, la historia clínica. Esto se traduce en el marco del Régimen de Protección de Datos, en la facultad que les asiste a los individuos como sujetos de derechos de ejercer control sobre la información personal que le concierne, y en especial en lo que tiene que ver con los datos relativos a su salud, que, para la normatividad vigente, son clasificados como datos sensibles, y especialmente protegidos por nuestra legislación.

1.2 Aportes Normativos Sobre el Régimen de Protección de Datos en Colombia

El régimen de protección de datos personales consagrado en la Ley 1581 de 2012, expedida por el Congreso de Colombia, "por medio de la cual se dictan las disposiciones generales para la protección de datos", establece en su ámbito de aplicación que sus principios serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. (Congreso de Colombia, ley 1581, 2012, art. 2).

En esta línea de argumentación, podría pensarse que, en Colombia, esta ley desarrolla el derecho Constitucional que tienen todos los sujetos para que su información personal contenida en bases de datos públicas o privadas sea susceptible de ser modificada en cualquier

momento; y en tal sentido, como es natural, otorga a las personas naturales unos derechos de actualización, acceso y rectificación de la información.

Esta disposición establece el derecho que tienen los usuarios del sistema de salud en Colombia a que se protejan sus datos personales en lo que respecta a la libre circulación de su información por medios digitales y automatizados, especialmente en lo que tiene que ver con la transmisión de los datos personales y la garantía de los titulares de que en dicho proceso se respeten sus derechos fundamentales a la intimidad, buen nombre, habeas data, privacidad, y a la protección de los datos.

1.3 Aportes Jurisprudenciales Sobre el Régimen de Protección de Datos en Colombia.

La Corte Constitucional, al hacer alusión al derecho fundamental al habeas data y los principios que gobiernan la administración de los datos, establece que en el tratamiento del dato personal y las garantías constitucionales que amparan el derecho a la protección de la información,

> El controlador de la base de datos está llamado a aplicar en debida forma los principios que gobiernan la administración de los datos personales (entre los que destacan, para efectos de este caso, los principios de libertad, transparencia y acceso), pues la garantía efectiva del derecho fundamental al habeas data está asociada, entre otras, a su cumplimiento. (Sentencia SU139/14, 2021).

Bien pareciera por todo lo anterior, que el legislador en su teoría, propone una articulación de principios que en consonancia con la Constitución Política de Colombia, impone a los operadores de salud, en su calidad de Responsables del tratamiento de los datos, garantizar un valor a la información de los usuarios, desde una mirada ética médica, el

cumplimiento normativo, y la responsabilidad demostrada; particularmente mediante la aplicación de códigos de autorregulación y buenas prácticas en el acceso, utilización y circulación de la información, que en la realidad, den cuenta de la licitud, lealtad y transparencia hacia las personas cuyos datos personales están tratando los operadores de salud, en aras de asegurar los derechos fundamentales de los beneficiarios del servicio.

Resultados

Llegando a este punto, es preciso abordar en este estudio los principios orientadores del Régimen de Protección de Datos para el quehacer del profesional en salud en Colombia.

En este sentido, es oportuno definir estas afirmaciones regulatorias fundamentales, para el desarrollo integral de este reglamento de protección de datos:

2. Principios Orientadores del Régimen de Protección de Datos.

En el marco general de la ley 1581 de 2012, por medio de la cual se dictan las disposiciones para protección de los datos personales, se establecen los principios orientadores para la protección del derecho fundamental a autorizar la información personal para su posterior actualización y rectificación.

Estos principios esenciales para proteger los derechos de los titulares de la información en cuanto al tratamiento de los datos en Colombia, y otros países comprometidos con los estándares internacionales de Protección de datos y Privacidad, fundamentan la parte estructural del sistema jurídico, en tanto cumplen una función, e integración del ordenamiento normativo.

Así las cosas, es necesario determinar un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de los derechos de los titulares, los cuales permitirán a los profesionales de la salud dar cumplimiento a lo establecido en la Ley 1581 de 2012, y abstenerse de llevar a cabo tratamientos no compatibles con su labor en ejercicio actividades relacionadas exclusivamente con la vida privada y familiar de los usuarios del sistema de salud.

En este sentido, a través de la norma citada, se definen los principios rectores como aquellos que permiten a los responsables y Encargados del tratamiento del dato personal, el cumplimiento reglamentario y la responsabilidad proactiva, la cual demanda de esta disposición y de quienes acceden a la información, que los datos sean tratados de manera lícita, leal, transparente y no sean transferidos a terceros sin las condiciones de seguridad adecuadas.

2.1 Responsabilidad Demostrada (Acountabillity).

La responsabilidad demostrada (Acountabillity), en el tratamiento del dato personal, es entendida como aquel principio que requiere de los Responsables y Encargados de administrar los datos, la implementación de acciones tendientes a adoptar medidas apropiadas, efectivas y verificables, respecto a la ejecución de las normas sobre protección de datos, así como exige de los sujetos obligados, estar en capacidad de evidenciar la correcta realización de sus deberes y demostrar el compromiso para ejecutar las políticas y protocolos de administración de datos.

Bien pareciera por lo dicho anteriormente, que el “compliance” como determinante de garantizar la Responsabilidad Demostrada, representa la creación de modelos de prevención y

manejo de riesgos, “que, a través de la introducción de una cultura del respeto de las normas legales y éticas en las empresas, establecen códigos de conducta, medidas de auto vigilancia, controles y la determinación de los flujos de información”. (Cabezas, 2023, p.12).

Estas nuevas exigencias del derecho, conllevan a que los operadores de salud incorporen en sus políticas de privacidad las mejores prácticas en el establecimiento de códigos de ética y conducta, que garanticen las medidas organizativas, técnicas, humanas y administrativas necesarias para cumplir con los demás principios consagrados en el Régimen de Protección de Datos Personales y la garantía de los titulares de preservar su derecho a la intimidad, al buen nombre, y a la protección de la información.

Su importancia trasciende pues al deber legal, y obliga a los actores a mantener la debida diligencia para proteger y asegurar los derechos y libertades de las personas, así como promover el respeto por la vida privada y la protección de los datos personales, cuyo propósito radica en proteger la autonomía y dignidad humana.

2.2 Principio de Finalidad.

En cuanto al principio de finalidad en materia de protección de datos personales; este revela que la utilización de los datos de un titular, solo se debe dar en casos autorizados de manera previa, expresa e informada por este, cumpliendo con una finalidad legítima y destinada a realizar los fines exclusivos para los cuales fue entregada por el titular.

Al respecto, la Superintendencia de Industria y Comercio, en varios pronunciamientos ha indicado que en el principio de finalidad para el tratamiento de los datos personales, es necesario tener en cuenta el literal b) del artículo 4 de la Ley 1581 de 2012, el cual

determina que: "el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular" (Congreso de Colombia, ley 1581, 2012, art. 4), al momento de solicitar la autorización para realizar el tratamiento de los datos personales.

Con el fin de interpretar mejor, y entrar en armonía con este precepto, se hace necesario examinar atentamente el decreto que regula parcialmente la Ley 1581 de 2012, el cual pretende que en la recolección de los datos personales se garantice la finalidad para lo cual es recolectada la información y esta no sea utilizada para fines diferentes a los informados al titular. (Decreto 1377, 2013, art. 4).

En consecuencia con este principio, y valorando lo que en este punto interesa, es preciso manifestar que el profesional de la salud en su intervención profesional ha de garantizar lo reglado en esta materia al momento de realizar el tratamiento de la historia clínica, en el entendido de que esta, es el registro obligatorio de las condiciones de salud del paciente, por lo que solo podrá ser tratada conforme al estricto cumplimiento de lo establecido en la Ley de protección de datos personales y sus decretos reglamentarios.

Añádase pues que, como actividad reglada, el profesional en salud solo puede ejercer el tratamiento del dato personal, si esta obedece a una finalidad legítima, con el consentimiento previo, expreso e informado del paciente, que podrá obtener a través de la debida autorización del titular, la cual deberá solicitar a más tardar en el momento de recolección de sus datos personales para dar estricto cumplimiento al principio de finalidad y demás garantías Constitucionales.

2.3 Principio de Libertad.

Según lo define la ley 1581 de 2012, en su artículo 4, el principio de libertad en el tratamiento del dato personal es aquel que sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Bajo este supuesto de absoluta confianza y reserva que prima entre el profesional de salud y el paciente, se hace indispensable acoger el principio de libertad como aquel que condiciona y limita el acceso irregular, la divulgación no permitida, y la transmisión de los datos personales a un tercero en el evento en que por alguna razón el facultativo de la salud hicera un acceso o circulación de datos no justificada, sin que medie previa autorización del titular.

En la actualidad, este principio concede las garantías constitucionales al beneficiario de que sus datos personales no serán compartidos con terceras personas sin que medie su aprobación; y previene contra los abusos que pueden llevar a cabo los galenos y en general el equipo de salud, al momento de realizar el tratamiento de los datos personales; así como permite elegir a los individuos voluntariamente si su información personal puede ser utilizada o no en bases de datos clinicas. Tambien impide que la información sensible previamente registrada pueda pasar a otro que la utilice para fines distintos para los que fue autorizado inicialmente.

Así las cosas, en el ejercicio de garantizar los derechos y las libertades de las personas, existen algunas excepciones que en algún momento pueden considerar los profesionales de la salud para imponer una injerencia en los derechos garantizados. Se trata pues, de las

exclusiones que taxativamente contempla la Ley de Protección de Datos en los casos en que sea necesario acceder y tranmisitir la información consignada en la historia clinica sin que exista previa autorización del paciente.

Se trata indiscutiblemente de lo preceptuado en la Ley Estatutaria de protección de datos, la cual en su artìculo 10 establece: "La autorización del titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, siempre que se refiera a asuntos administrativos, legales o judiciales, que por su naturaleza, requieran que el profesional en salud, acceda y transmita la historia clinica a terceros, sin previa autorización del dueño de la información, y en cumplimiento del mandato legal. b) Casos de urgencia médica o sanitaria. No será necesaria la autorización para el acceso a la información cuando el procesamiento de los datos por parte del operador de salud, este indique cualquier condición que requiera atención inmediata que comprometa la vida o integridad del usuario de salud. c) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos", siempre que por su relevancia medica, sean utiles a la Nación. (Congreso de Colombia, ley 1581, 2012, Art 10).

No obstante, puede determinarse que este tipo de prácticas no pueden ser deliberadas y obedecen excepcionalmente a los casos previstos en la Ley. Ningún profesional podrá invocar la injerencia a la documento clínico, sin que esta que esta responda a una necesidad acuciante y en especial que obedezca a un fin legitimo que persiga.

2.4 ***Principio de Veracidad o Calidad.***

Añadase a este estudio este principio el cual hace referencia a que los datos personales sólo pueden tratarse para finalidades explícitas y legítimas para los cuales fueron recogidos los datos.

En el marco jurídico Colombiano, el principio de veracidad y calidad se encuentra establecido en el numeral d) del artículo 4 de la Ley 1581 de 2012, y se entiende como aquel que condiciona la información que se encuentra sujeta al Tratamiento del dato e indica que esta debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

A primera vista la interpretación de este principio, nos lleva a determinar que es imperativo proteger la información de la salud catalogada como sensible, la cual se encuentra registrada en sistemas informáticos, bajo las medidas de seguridad adecuadas y respaldando la debida diligencia.

Por mandato legal, todas las empresas sean públicas o privadas, les asiste el deber de garantizar la veracidad de la información que reposa en sus bases de datos automatizadas o físicas, por lo que es necesario crear un conjunto de mecanismos que en articulación con el principio de confidencialidad promuevan el acceso y la transparencia en la información.

Los desafíos que trae aparejada la búsqueda de estrategias para garantizar este principio nos invita a pensar en la adopción de instrumentos normativos y técnicos que faciliten al profesional en salud implementar pautas y normas de seguridad en los sistemas de información tendientes a crear una cultura de manejo de datos confiable y segura, que de

cara al paciente, posibilite decidir sobre sus datos y optar por actualizarlos, modificarlos o borrarlos conforme a las garantías que ofrece la Ley de Protección de Datos.

2.5 Principio de Transparencia.

Admitamos que con todo lo dicho hasta aquí, y con el fin de avanzar en la descripción de los principios orientadores para la protección de los datos personales, que se hace necesario y no menos importante, enunciar el principio de transparencia en el tratamiento del dato personal.

Al respecto es preciso indicar que este hace referencia a la obligación del Responsable o el Encargado del tratamiento de que en cualquier momento dé respuesta sin ninguna restricción acerca de la existencia de los datos que le conciernan al titular. (Ley 1581,2012, art. 4, numeral e). Para el caso objeto de estudio, este principio describe la importancia de que en el sector de la salud, se respalden los derechos de los usuarios, y en su lugar, se avale este principio como medio para obtener de los actores del tratamiento del dato, en cualquier momento, y sin restricciones, información acerca de los datos que le conciernan al titular.

La transparencia es uno de los principios fundamentales en el manejo de la información, por tal razón las entidades privadas y públicas deberán implementar las medidas de seguridad apropiadas y efectivas para proteger la información tratada, en procura de proteger los derechos humanos de los pacientes, de modo tal, que estos puedan tener acceso a su historia clinica sin dilaciones, buscando blindar la seguridad, e impedir que personas no autorizadas accedan al documento clinico catalógado como sensible. Para ello deberán

contar con las medidas organizativas que eviten su adulteración, perdida, consulta, uso o acceso no autorizado.

2.*6 Principio de Acceso y Circulación Restringida.*

El principio de acceso y circulación restringida de la información, guarda una estrecha relación con la doctrina de la transparencia, que en todas las instancias busca como lo señala el numeral f) de la nombrada Ley de Protecciòn de datos, lograr que:

> El Tratamiento sea sujeto a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. Y en este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley, (Congreso de Colombia, ley 1581, 2012, art. 4).

Es así como el acceso a la historia clinica se interpreta en el estricto sentido de la Ley Estatutaria de protecciòn de datos, como aquella actividad del profesional que genera unos deberes y obligaciones para los agentes del sistema de salud, en cuanto los obliga a respetar su naturaleza privada y el sometimiento a reserva que unicamente puede ser conocido por terceros previa autorizaciòn del titular de la informaciòn o en los casos previstos por ley.

Este argumento evidencia claramente el propósito del creador del Régimen de Protección de Datos personales, al considerar en su génesis una concepción garantista y Constitucionalista en la administración de los datos personales.

En la actualidad, sin embargo, se presenta el debate respecto al manejo de la información; esto es, el dilema por el acceso y la circulación restringida del documento clínico,

especificamente en lo que tiene que ver con la historia del paciente, ya que esta práctica va mas allá de las disposiciones de la ley, y los principios de la administración de los datos, y cuestiona la relación existente entre el deber de informar y la garantía de conocer y conceder los límites respecto del acceso a la información medica y la restricción al momento de hacer la entrega por razón del servicio o por petición del titular.

Estas consideraciones claramente comprometen la autonomía de los prestadores de salud y plantea el debate acerca de la responsabilidad de quienes participan en el acceso y circulación de la historia clinica, siempre que obedecer a este principio en todo momento, representa un riesgo mayor de violación a las normas medicas, y de manejo de la historia clinica.

2.7 Principio de Seguridad.

Partiendo de la definición normativa, se entiende este principio como aquel que obliga a que en "la información sujeta al Tratamiento por parte el Responsable o del Encargado de administrar los datos, se implementen medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros" (Congreso de Colombia, ley 1581, 2012, Art. 4).

El impacto de las tecnologías y las comunicaciones, ha demandando de las entidades vigiladas unas obligaciones, y mayores exigencias para quienes tienen a su cargo la responsabilidad de proteger la información que reposa en las bases de datos automatizadas o físicas, así lo indican los mandatos reglamentarios en materia de seguridad de la información.

En esta era digital, los datos se han convertido no solo en un activo valioso, sino estratégico de las organizaciones, y estos pueden ser protegidos de muchas maneras,desde un adecuado nivel de protección que contemplan los atributos de confidencialidad, integridad y autenticidad.

Es menester comprender còmo el derecho, como disciplina, puede aportar al cumplimiento de este principio de seguridad, y para ello citaremos a Velasco (2008), quien desde una mirada crítica nos dice:

> La trascendencia de la seguridad de la información en las organizaciones públicas o privadas radica en que: (i) el volumen de información crece día a día; (ii) la información es un intangible con un valor bastante apreciable en la economía actual; (iii) la información es una ventaja estratégica en el mercado, que la convierte en algo atractivo para la competencia, como elemento generador de riqueza (p.338).

En sano criterio, es conveniente precisar que lo expuesto por el autor no desconoce la realidad que hoy en día se vive en las entidades privadas y públicas al darle un menor valor a la información. No obstante con la incorporación de nuevas leyes, y las exigencias del Ente de Control (Superintendencia de Industria y Comercio), estas organizaciones se han visto en la obligación de crear sistemas de gestión para garantizar la seguridad en los procesos que implican incorporar las mejores prácticas profesionales y administrativas, para respaldar que los datos recopilados sean correctos, y no puedan ser manipulados por otros, así como que solo las personas con accesos autorizados a los datos personales los procesen, y que a traves de la creación de políticas y procedimientos puedan mitigar los

riesgos, adoptando medidas administrativas, técnicas, y humanas preventivas que salvaguarden la información de los titulares.

En esta investigación, pensar en el principio de seguridad constituye un mayor desafío por parte de las Entidades sanitarias para crear sistemas de gestión de seguridad de la información que contrarresten las amenazas, vulnerabilidades y riesgos que atenten contra la seguridad de la información, así como el logro de procesos que preserven la confidencialidad, integridad y disponibilidad de los datos al interior de la compañía.

2.8 Principio de Confidencialidad.

Este principio por excelencia nos indica que "todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información" (Congreso de Colombia, ley 1581, 2012, art 4).

Tradicionalmente el principio de confidencialidad, visto desde la optica medica en el marco de la excelencia profesional, ha significado una mayor conciencia de los deberes eticos del profesional en salud respecto a la relación con el paciente, ligazón que entre muchas cosas se caracteriza por garantizar la reserva de la información a la cual tiene acceso el profesional sanitario en ejercicio de su labor.

Es preciso manifestar que el "El secreto profesional médico constituye garantía constitucional de imperioso cumplimiento para el idóneo desarrollo de las ciencias de la salud y para la prevalencia de determinados derechos fundamentales, inherentes a toda persona" (Portilla, 2019, p.1).

Su aplicación representa un deber que el profesional sanitario debe cumplir invariablemente, evitando que la información que conociere en razón de su profesión, sea divulgada a terceros, sin previa autorización del titular, salvo en excepciones legales.

El deber de guardar la confidencialidad entre la relación galeno-paciente, por momentos genera algunas tensiones en el deber de confidencialidad, en cuanto este primero se ve enfrentado a una serie de eventualidades que en ocasiones van en contravía del marco legal que como bien lo refiere Portilla, (2019), en circunstancias en que compartir la información con un tercero discrepa con el carácter personalísimo de aquella figura que permite la relación de confidencialidad inescindible como derecho del paciente.

> La información obtenida por el médico en el ejercicio de su profesión se encuentra privilegiada por el secreto profesional, en virtud de su derecho-deber de guardar confidencialidad sobre la información a la que tenga acceso en su condición de profesional de la salud, por ende, no puede ser molestado ni sancionado por guardar el secreto médico, todo lo contrario, solo podría ser amonestado en caso de su revelación. Corte Interamericana de Derechos Humanos (2004). (Portilla, 2019, p 357-386)

La supremacía de este principio permite comprender el grado de dificultad que debe afrontar el profesional de salud, al momento de ponderar las regulaciones en materia de protección de datos y los derechos y obligaciones que le asisten a los usuarios del sistema del salud, siempre que este principio no puede considerarse absoluto en la garantía de los derechos constitucionales de las personas.

Sin embargo, al llegar a este punto, es necesario resaltar que en cuanto a este principio de confidencialidad se refiere, existen unos elementos que le dan valor a la información personal y obliga asegurar las mejores practicas en el manejo de la información por quien accede a la historia clinica como quien està obligado a conservar el secreto profesional, aun despues de finalizada su relación con la intervenciòn del conocedor.

3. Discusión

Para profundizar en los fines de este artículo, se hace necesario delinear los desafíos que presenta el personal del área de la salud al momento de aplicar la ética deontológica y la interoperabilidad, en relación con el cumplimiento del régimen de protección de datos personales en su quehacer profesional.

Ahora bien, para abordar estos objetivos se presentará la discusión en dos apartados, a saber:

3.*1 Ética Deontológica*

La ética deontológica, entendida esta, segùn lo define Hincapié (2021), como un “conjunto de principios y reglas que han de guiar una conducta profesional” (p. 214), no regula la actuaciòn del profesional en salud, siempre que este para cumplir con sus propòsitos, ha de acogerse a los preceptos morales y deontològicos consagrados en sus propios códigos, poniendo de manifiesto, la necesidad de proyectar valores eticos que realmente orienten su actuar profesional. Esto es, en la pràctica, la formaciòn de la personalidad profesional de los operadores de salud, que para dar caval cumplimiento al règimen de protecciòn de datos, han de tener en cuenta los preceptos constitucionales, normativos y jurisprudenciales que en esta materia imparta el legislador.

3.2 *Desafíos que Presenta el Personal del Área de la Salud al Momento de Aplicar la Ética Deontológica*

En el marco del estudio que se adelanta en relación con el Régimen de Protección de datos personales y el desafío que supone este sistema para la creación de la historia clínica, y la ética de los profesionales de salud, es preciso soportar la teoría deontológica comprendida como aquellos códigos morales y de conducta que deben adoptar los profesionales en desarrollo de su actividad.

Para nadie es un secreto que la implementación del Régimen de Protección de Datos Personales trajo consigo un sin número de aportes y desafíos que, al momento de proteger los derechos y garantías constitucionales de los usuarios de salud, situaron a esta estructura sanitaria en una disyuntiva en todo en lo que tiene que ver con la intervención de los profesionales al momento de tratar la historia clínica y acceder a los sistemas informáticos.

Los reglamentos de protección de datos personales han limitado la labor de los expertos en salubridad, siempre que con sus lineamientos problematizan la relación entre el derecho, las tecnologías y la ética.

La conexión entre moral, derecho, y sistemas informáticos, trae consigo una serie de tensiones en cuanto a la cautela que tienen los profesionales respecto a la capacidad de los sistemas, los derechos de las personas que se pueden ver afectados por las nuevas tecnologías, la interoperabilidad, y las limitaciones que trae consigo la ley para el ejercicio del profesional de salud, así como las vulnerabilidades que puedan presentar los nuevos

desarrollos al momento de acceder, intercambiar, y utilizar la información clínica, cambiando de este modo la forma en que se hacen las cosas.

Las implicaciones éticas de la ciencia y las tecnologías para los deberes y responsabilidades de los profesionales en salud ponen en evidencia el conflicto entre ética, derecho, y cómo finalmente estas disciplinas afectan bienes jurídicos como la privacidad, la intimidad, la libertad, en otros.

Considerar estas coyunturas puede llevar a determinar los desafíos que presentan los profesionales del área de la salud al momento de garantizar sus códigos éticos y el cumplimiento del Régimen de Protección de Datos Personales en su ejercicio profesional, desde la obligación legal de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, hasta entender que por el hecho de ser operador de la salud, no está facultado a conocer información confidencial del consultante, sin que tenga relación una estrecha relación profesional.

Para ilustrar mejor lo dicho anteriormente, resulta pertinente recordar a Maldonado (2020, quien en su escrito el derecho disciplinario ético-profesional y su lugar en el ordenamiento jurídico Colombiano, hace una reflexión en cuanto a la necesidad de inspección y vigilancia de los profesionales, y acude al derecho disciplinario como “fuente que parte de la regulación que el legislador expide para el ejercicio de una determinada profesión u oficio, con el fin de proteger a la sociedad del riesgo que aquella puede representar” (p.7).

Como resultado de lo anterior, se puede colegir que la conducta del profesional en salud, es determinante al momento de cumplir la responsabilidad social, los principios morales y normativos que trae la Ley de Protección de Datos Personales, y el deber de realizar

acciones racionales orientadas a no hacer daño y asegurar el bien general, y finalmente pero no menos importante, es fundamental, la vigilancia y control sobre todo aquello que tenga relación con la historia clínica y el deber de mantener la reserva y confidencialidad de la información.

3.3 Interoperabilidad de la Historia Clínica.

Desde la óptica de la historia clínica en Colombia, entendida como aquel documento privado que goza de la restricción de reserva legal por comprometer derechos fundamentales de los titulares, en su proceso sistemático y garantista de la protección de la privacidad, y la custodia de la información, nace la necesidad de instaurar la interoperabilidad como medio de evolución de los registros médicos; aquella que pretende evitar la adulteración, perdida o destrucción de manera intencionada de la información por quienes tienen el deber legal de garantizar el secreto profesional.

Un breve recuento por la gobernanza digital permite plantear el interrogante acerca de lo que representa la interoperabilidad para el profesional de la salud al momento de acceder y transmitir la información contenida en la historia clínica, así como contraponer la garantía de los derechos fundamentales de los titulares de los datos.

Un marco normativo escaso que limita el quehacer del profesional que tiene acceso a la historia clínica, da cuenta de los pocos o nulos esfuerzos realizados por los gobiernos para institucionalizar políticas públicas que den solución al conflicto que se presenta entre los códigos, que regulan el quehacer deontológico del profesional en salud y la transmisión de los datos personales con terceras personas, que se involucran en el tratamiento del dato

y el estricto cumplimiento del régimen de protección de datos personales que le asiste a las instituciones prestadoras de salud.

Tener una visión holística de este dilema, y su incidencia en la trazabilidad, confidencialidad e integridad de la información relacionada directamente con la privacidad e intimidad de los pacientes,

> Demanda de las instituciones públicas y privadas un mayor esfuerzo para la puesta en marcha de iniciativas desde distintas disciplinas que permitan la fianza de los derechos fundamentales de quienes acceden al servicio de salud con la firme convicción de que en la prestación de los servicios se les protege y respalda su intimidad y privacidad personal y familiar (Contreras, 2020, p 97)

Precisamente y pretendiendo garantizar los atributos de la información, quien acceda al registro de atención médica deberá cumplir con el principio fundamental de confidencialidad, por medio del cual se respalda el deber del secreto profesional, y la no divulgación de los datos personales almacenados o en tránsito dentro de la estructura de salud.

En tal sentido, y “Como lo señala la norma, su tratamiento debe estar fundamentado en el ordenamiento y garantías jurídicas desde los principios del tratamiento de datos personales y en especial de datos sensibles como los son los datos de salud” (Buitrago, 2023, p. 3).

Con la entrada en vigencia del Reglamento General de Protección de Datos, ha de interpretarse la interoperabilidad en las historias clínicas desde el buen uso razonable de los datos, y el cumplimiento de las disposiciones generales de protección de datos, obedeciendo a una finalidad legítima que solo puede ejercerse con el consentimiento previo, expreso e

informado del titular y con la certeza de que la información tratada obedece al principio de veracidad o calidad de los datos, desde la aplicación de medidas técnicas, humanas y administrativas, necesarias para otorgar infalibilidad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

El Régimen de Protección de Datos Personales en Colombia, como norma garantista de derechos fundamentales se encuentra regulada en la Ley 1581 de 2012, sus decretos reglamentarios, y la Constitución Política. Estas disposiciones legales pensadas en principio para reconocer derechos de las personas como la intimidad, la protección de los datos, el buen nombre y demás, con el paso del tiempo, han marcado un hito en cuanto los avances y desafíos que han tenido que afrontar los profesionales de salud al momento de abordar la historia clínica y garantizar los derechos constitucionales de sus titulares.

Este régimen especial, por su naturaleza estatutaria, obliga a todos los sectores públicos y privados a implementar sus principios y acoger las instrucciones que en tal sentido imparta la Superintendencia de Industria y Comercio.

No obstante lo anterior, se puede percibir en la investigación realizada, los grandes vacíos en cuanto a políticas públicas se refiere en materia de protección de datos personales, si consideramos que pese a que existen grandes avances tecnológicos en esta materia, y estos han surgido como alternativa para garantizar la interoperabilidad de la historia clínica, y el cumplimiento del Régimen de Protección de Datos Personales, aun se evidencia una visible ausencia de intervención del Estado como autoridad pública para crear regulaciones y acciones que de manera específica contrarresten los riesgos de violación por parte de los operadores de salud de los derechos de los titulares al

momento de intercambiar los datos médicos relevantes (historia clínica), por cuanto en el proceso de transmisión de la información se puede presentar la perdida de privacidad, confidencialidad y garantía de los principios consagrados en la constitución política y la ley de protección de datos. .

Ante el incumplimiento de las disposiciones consagradas en la Ley de protección de datos y sus decretos reglamentarios, la Superintendencia de Industria y Comercio como Ente de control podrá adoptar las medidas sancionatorias necesarias para proteger a los administrados.

Este régimen disciplinario, asociado a los códigos de conducta del profesional en salud establecidos en la Ley 1164 de 2007, han hecho de la práctica sanitaria, un desafío para la garantía de los derechos de los beneficiarios del sistema de salud, toda vez que la incorporación de nuevas tecnologías, el deber de cumplir con el mandato legal, y la ética deontológica, contrario a servir como instrumento para una protección integral de los derechos que se tutelan, han encontrado indudablemente desaciertos en la reserva de la información y el tratamiento de los datos personales; especialmente los datos sensibles, la creación de mecanismos de autorregulación institucional, y las limitaciones propias que trae consigo la escasa regulación que en esta materia tiene Colombia.

En lógica con lo dicho hasta aquí, se pudo evidenciar que existe un conflicto determinado entre el derecho a la protección de los datos personales, el uso y aplicación de las nuevas tecnologías y los códigos de conducta que regulan a los profesionales de salud, siempre que estas tres áreas en sí mismas, y en asocio, no garantizan en su totalidad la libertad e igualdad en los derechos fundamentales de las personas.

Sin embargo, pese a los desafíos que trae consigo la nueva era digital y la escasa normativa respecto a la interoperabilidad; no se puede pasar por alto la importancia y grandeza de este sistema como soporte del documento clínico que genera una cultura de responsabilidad, propicia un mejor desempeño de los operadores de salud, brinda ventajas en los sistemas de información en los cuales se contienen el historial médico asistencial y preserva los derechos fundamentales a la salud, la intimidad, la protección de los datos y el habeas Data.

4. Referencias

Arbeláez, J. M. B., & Cuesta, D. L (2015). El secreto profesional en Colombia, regulación y sanciones por su revelación; *Dos mil tres mil*, (17), 46-51. https://revistas.unibague.edu.co/dosmiltresmil/article/view/20

Aguilar, M. (2018). La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados. [Tesis de pregrado] Universidad Católica de Colombia Sede Bogotá

Alvarado, D. J. B. (2019). La historia clínica: algunos comentarios desde la medicina y el derecho. *Verba luris*, 14 (42), 153162

https://revistas.unilibre.edu.co/index.php/verbaiuris/article/view/5665/5277

Bernal-Acevedo, O., & Forero-Cam acho, J. C. (2011). Sistemas de información en el sector salud en Colombia. *Revista Gerencia y políticas de salud*, *10*(21), 87-97.

https://revistas.javeriana.edu.co/index.php/gerepolsal/article/view/2590

Buitrago-Botero, D. M. (2023). Rastreo normativo de la historia clínica electrónica en Colombia. *Ratio Juris*, *18*(36), 307. D.O: 10.24142

Cabezas Azuero, J. S. (2023). Tratamiento de datos personales y compliance en Colombia. *Revista de la Facultad de Derecho y Ciencias Políticas, 53*(138), 12. Htpps://orcid.org/0000-0002-2431-9417

Calle, S. B. (2009). Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia. *Precedente Revista Jurídica*, 8 (8), 120-128. https://dialnet.unirioja.es/servlet/articulo?codigo=9015856

Contreras, A. F. (2020). 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, 29*, (04) 95-116 D.O: /10.18601/1657195

Congreso de Colombia (octubre 17 de 2012). Por medio de la cual se dictan disposiciones para la protección de datos personales. [Ley 1581 de 2012]. D.O: 48.587.

Constitución Política de Colombia, (1991). Constitución política de Colombia - 2015.pdf (corteconstitucional.gov.co)

Corte Constitucional (26 de abril de 2022). Sentencia 143/22 M.P Alejandro Linares Cantillo.

Chávez, L. A. M. (2012). Normas corporativas vinculantes y transferencias internacionales de datos personales: elementos para su reglamentación. *Revista de Derecho*, Comunicaciones y Nuevas Tecnologías, (8), pág. 6-16. https://dialnet.unirioja.es/servlet/articulo?codigo=7505134

Chen Mok, S. (2010). Privacidad y protección de datos: un análisis de legislación comparada. Diálogos *Revista Electrónica de Historia*, 11(1), 116-133 https://www.redalyc.org/articulo.oa?id=43915696004

Decreto 1377, (2023). Art 4. República de Colombia. Decreto 1377 de 2013 - Gestor Normativo - Función Pública (funcionpublica.gov.co).

Díaz, A. M. C., & Arias, A. V. (2016). Responsabilidad social y ética médico-sanitaria. *Ratio Juris UNAULA*, 11(22), 80-85

https://publicaciones.unaula.edu.co/index.php/ratiojuris/article/view/79

Eslava-Rincón, J. I., Camelo-Tovar, F. A., Mina-Rosero, L., Vásquez-Candia, M. E., & Mejía-Rocha, M. M. (2018). Análisis de la capacidad de respuesta de los sistemas de información en salud para la supervisión de riesgos que afectan el derecho a la salud en Colombia. *Revista Gerencia y políticas de salud*, 17(35), 7-12.

https://revistas.javeriana.edu.co/files-articulos/RGPS/17-35%20(2018-II)/54557477011/

Etreros-Huerta, J., Marco-Cuenca, G., Abad-Acebedo, I., & Muñoz-Montalvo, J. F. (2009). La interoperabilidad como base de la Historia Clínica Digital del Sistema Nacional de Salud. *Todo Hospital*, 2009(junio), 467-474

http://eprints.rclis.org/3856/1/hcdsns_semantic.pdf

Flórez -Rojas, M. L. (2022). *El determinismo algorítmico en Colombia: riesgos para la protección del usuario. Derecho de las tecnologías y las tecnologías para el derecho*, Ediciones Uniandes

García-González, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. Boletín mexicano de derecho comparado, 40(120), 743-778

https://www.scielo.org.mx/pdf/bmdc/v40n120/v40n120a3.pdf

Garriga, A. (2012). VIH y derechos fundamentales: el derecho a la protección de datos personales y el registro obligatorio de los portadores del VIH en España. [programa Cosolider- Ingenio] Universidad Vigo sede España

Gómez, C. A. (2002). Dogmática del derecho disciplinario. Universidad Externado de Colombia.

Gutmann, T. (2019). Dignidad y autonomía. Reflexiones sobre la tradición kantiana. *Estudios de filosofía*, (59), 233-254

http://www.scielo.org.co/pdf/ef/n59/0121-3628-ef-59-00233.pdf

Hernández Leal, E., Duque- Méndez, N., & Moreno-Cadavid, J. (2017). Big data: una exploración de investigaciones, tecnologías y casos de aplicación, (20), 15-38 https://www.redalyc.org/journal/3442/344251476001/html/

Mazo, M. (2014). El bioderecho: La respuesta jurídica a los problemas que plantea la biótica. [proyecto de investigación El concepto de persona puente entre la bioética y el derecho] Corporación Universitaria Uniremington Colombia

http://www.scielo.org.co/pdf/pml/v9n2/v9n2a07.pdf

Mazo, H. M. (2021). Fronteras del bioderecho y la bioética., *Revista Principia Iuris*, 18(38), 42-50 http://revistas.ustatunja.edu.co/index.php/piuris/article/view/2486/2062

Ley 1581, (2012). Art. 2 y 4. República de Colombia. Ley 1581 de 2012 - Gestor Normativo - Función Pública (funcionpublica.gov.co)

Lima, H. J. S. (2022). Nuevas tecnologías, protección de datos personales y el seguro. *Revista Ibero-Latinoamericana de seguros, 31*(57) 249-270 D.O: 0.11144.

Lopera, M., (2022). Retos éticos para los administradores en salud en la época contemporánea. *Revista Facultad Nacional de Salud pública,* Vol 40 (1), pág. 2-9. D:O: 10.17533.

López-Torres, J. (2014). Antecedentes internacionales en materia de privacidad y protección de datos personales. *Ejil-EAFIT Journal of International Law, 5*(2), 109.

https://core.ac.uk/download/pdf/290651897.pdf

Maqueo-Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de derecho (Valdivia)*, 30(1), 82-91.

https://www.scielo.cl/pdf/revider/v30n1/art04.pdf

Martínez, C. A. C. (2013). Límites al derecho de acceso a la información clínica en los casos de estado necesidad terapéutica y anotaciones subjetivas. Especial referencia al sistema español. *Via Inveniendi Et Iudicandi*, *8*(2), 34.

https://www.redalyc.org/pdf/5602/560258674003.pdf

Melo, V., & Hernando, A. (2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. *Revista de derecho*, (29).

http://www.scielo.org.co/pdf/dere/n29/n29a13.pdf

Mendoza, A. (2017). La relación médico paciente: consideraciones bioéticas. Revista peruana de ginecología y obstetricia, 63(4), 555-564.

http://www.scielo.org.pe/pdf/rgo/v63n4/a07v63n4.pdf

Narro-Robles, J., Rodríguez-Domínguez, J., Viesca-Treviño, C., & Abreu-Hernández, L. F. (2004). Ética y salud: Retos y reflexiones. Gaceta médica de México, 140(6), 663-665.

https://www.scielo.org.mx/pdf/gmm/v140n6/v140n6a17.pdf

Ojeda-Bello, Z. (2015). El derecho a la protección de datos personales desde un análisis histórico-doctrinal. Tla-melaua, 9(38), 58-70

https://www.scielo.org.mx/pdf/tla/v9n38/1870-6916-tla-9-38-00058.pdf

.Ornelas, L.G., & Higuera, M. (2013). La autorregulación en materia de protección de datos personales: la vía hacia una protección global. *Revista de Derecho, comunicaciones y nuevas tecnologías*, (9), 7-8.

https://Dialnet-LaAutorregulacionEnMateriaDeProteccionDeDatosPerso-7505127.pdf

Portilla-Parra, S. (2019). El secreto profesional médico y las personas con discapacidad, en el ordenamiento jurídico colombiano. *Revista socio-jurídico* 21 (2), 357-386.

https://revistas.urosario.edu.co/index.php/sociojuridicos/article/view/7591

Ramírez-López, S. (2015). Del campo de batalla a las calles: el derecho a la intimidad en la era de los drones. *Revista Derecho del Estado*, (35), 192-196.

https://revistas.uexternado.edu.co/index.php/derest/article/view/4339/4923

Ramírez-Torrado, M. L., & Aníbal-Bendek, H. V. (2015). Sanción administrativa en Colombia. universitas, (131), 111-117.

http://scielo.org.co/scielo.php?script=sci_arttext&pid=S0041-90602015000200004

Riascos Gómez, L. O. (2012). Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009. *Revistas jurídicas especializadas nacionales y extranjeras*. (20), 336-426

file:///C:/Users/usuario_51/Downloads/derechoyrealidad,+15_los_delitos_contra_los_datos_personales.pdf

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus: Revista Especializada en Sociología Jurídica y Política*, 8(1), 107. D.O: 10.14718

Ruiz Villarreal, I. F., & Morales Duque, C. (2021). Percepción de interoperabilidad de historia clínica electrónica HCE del profesional de salud del Hospital Regional Alfonso Jaramillo Salazar dl Líbano Tolima (Bachelor's thesis, Especialización en Auditoría y Garantía de Calidad en Salud).

Recuperado de: http://hdl.handle.net/10882/10955

Ruza, W., Valderrama, Y., & Leal, E. (2019). Elementos de la confidencialidad en el ejercicio profesional del auditor. *Cuadernos de Contabilidad*, 20(49), 5-17. D:O: 10.11144

Salvadori, I., (2011). De los delitos contra la confidencialidad, la disponibilidad y la integridad de los datos y sistemas informáticos regulación Española. *Novumjus*, 5 (1), 31-50.

https://novumjus.ucatolica.edu.co/article/view/684/702

Sánchez-Duque, J. A., Paredes-Mondragón, C. V., Ramírez-González, M. C., & Galvis-Acevedo, S. (2022). Historia clínica electrónica interoperable: El caso de

Colombia. *Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo*, 15(1), 153-154. D:O: 10.35434

Gómez-Córdoba, A., (2020). Dossier cuestiones bioéticas de la pandemia COVID 19. *Revista de biótica y derecho*, (50), 271-294

https://scielo.isciii.es/pdf/bioetica/n50/1886-5887-bioetica-50-00271.pdf

Corte Constitucional (2021, 14 de mayo). Sentencia SU 139 (Jorge Enrique Ibáñez Najar, M.P.). https://www.corteconstitucional.gov.co/relatoria/2021/SU139-21.htm

Sierra, G. A. M. (2020). El derecho disciplinario ético-profesional y su lugar en el ordenamiento jurídico colombiano. *Dixi*, (32), 1-44. D.O: 10.16925

Superintendencia de industria y comercio. Protección de datos. Ministerio de Comercio Industria y turismo. https: www.sic.gov.co/sities/default/files/files/boletin-jurídico/2017/17178735PDatos.

Tello, D. C. V. (2015). Implementación de tecnologías de la información y las comunicaciones (TIC) en Colombia. *Revista de Derecho*, Comunicaciones y Nuevas Tecnologías, (14), 5. D.O: 10.15425

Valencia-Agudelo, G. D., & Flórez Mazo, C. E. (2019). Metamorfosis de *la revista científica. De impresa a electrónica. Estudios Políticos*, (54), 9-13. D.O: 10.17533

Villacorta, M. (2022). Autocheking sobre una auditoría de SI RGPD. [Tesis de pregrado] Universidad Politécnica Sede Valencia

Winkler, M. I., Villarroel, R., & Pasmanik, D. (2018). La promesa de confidencialidad: nuevas luces para la investigación científica y la práctica profesional en salud mental. *Acta bioethica*, 24(1), 127-136.

https://www.scielo.cl/pdf/abioeth/v24n1/1726-569X-abioeth-24-01-00127.pdf