

UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE DERECHO

**MAESTRÍA EN DERECHO CON ÉNFASIS EN DERECHO INTERNACIONAL DE
LOS NEGOCIOS**

Rector: Juan Carlos Henao Pérez

Secretaria General: Marta Hinestrosa Rey

Decana de la Facultad de Derecho: Adriana Zapata Giraldo

Directora (e) del Departamento de Derecho de los Negocios: Adriana Castro Pinzón

Director Trabajo de Grado: Daniel Peña Valenzuela

Jurados: Juan Carlos Upegui
Sarah Osma Peralta

MARCO OCDE SOBRE GOBERNANZA DE LOS DATOS DE SALUD: APUNTES
PARA LA TRANSFORMACIÓN DIGITAL DEL TRATAMIENTO DE DATOS
PERSONALES DEL SISTEMA DE SALUD COLOMBIANO

ANGIE NATALY PEÑALOZA BENAVIDES

Director de tesis: Daniel Peña Valenzuela

UNIVERSIDAD EXTERNADO DE COLOMBIA
FACULTAD DE DERECHO
MAESTRÍA EN DERECHO INTERNACIONAL CON ÉNFASIS EN DERECHO
INTERNACIONAL DE LOS NEGOCIOS
BOGOTÁ
2019

CONTENIDO

INTRODUCCIÓN	5
1. TRATAMIENTO DEL DATO DE LA SALUD Y SU NIVEL DE PROTECCIÓN EN COLOMBIA	6
INTRODUCCIÓN.....	6
1.1. APROXIMACIÓN AL SISTEMA DE SALUD COLOMBIANO.....	6
1.1.1. Bases de datos de la salud.....	9
1.1.2. La historia clínica.....	13
1.2. DESAFÍOS DEL SISTEMA DE SALUD FRENTE AL TRATAMIENTO DE DATOS PERSONALES	17
1.2.1. Legislación aplicable al tratamiento de los datos personales.	18
1.2.2. Desafíos del sector salud.....	22
1.2.3. Ajustes que necesita el sector salud.....	24
CONCLUSIONES.....	26
2. TRATAMIENTO DEL DATO DE LA SALUD Y SU NIVEL DE PROTECCIÓN SEGÚN EL ESTÁNDAR OCDE	27
INTRODUCCIÓN.....	27
2.1. LOS DATOS DE LA SALUD SEGÚN LA OCDE.....	27
2.2. LA HISTORIA CLÍNICA ELECTRÓNICA EN PAÍSES OCDE	29
2.3. MARCO OCDE PARA LA GOBERNANZA DE LOS DATOS PERSONALES DE LA SALUD	31
2.3.1. Recomendaciones para la gobernanza de los datos personales de la salud.	32
2.3.2. Directrices OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.	42
2.3.3. Aplicación del marco OCDE a Colombia.....	43
CONCLUSIONES.....	44
3. LA PROTECCIÓN DEL DATO DE LA SALUD EN COLOMBIA FRENTE AL MARCO OCDE	45
INTRODUCCIÓN.....	45
3.1. NIVEL DE PROTECCIÓN DEL TRATAMIENTO DEL DATO DE LA SALUD EN COLOMBIA	46

3.2. TRATAMIENTO DEL DATOS DE LA SALUD EN COLOMBIA FRENTE A LA RECOMENDACIÓN OCDE.....	49
3.2.1. Compromiso y participación de una amplia gama de partes interesadas.	50
3.2.2. Coordinación y cooperación de las partes interesadas.....	51
3.2.3. Sistemas de datos de salud al servicio y protección del interés público.....	52
3.2.4. Información para las personas.	53
3.2.5. Mecanismos para consentir el tratamiento de datos.	54
3.2.6. Revisión y aprobación del uso de datos personales de salud para fines de investigación u otros de interés público relacionados con la salud.	55
3.2.7. Mecanismos públicos de información para que el tratamiento sea transparente.	55
3.2.8. Tecnología para la reutilización y el análisis de los datos.	56
3.2.9. Mecanismos de seguimiento y evaluación.....	57
3.2.10. Capacitación adecuada y el desarrollo de habilidades en medidas de privacidad y seguridad.....	58
3.2.11. Implementar controles y salvaguardas.....	59
3.2.12. Demostrar cumplimiento de expectativas nacionales sobre gobernanza de los datos de salud.....	61
3.3. AJUSTES PARA MEJORAR LA GOBERNANZA DE LOS DATOS DE LA SALUD EN COLOMBIA	62
CONCLUSIONES.....	66
BIBLIOGRAFÍA	67

INTRODUCCIÓN

Lograr los beneficios que pueden alcanzarse con el tratamiento de los datos de la salud, ha llevado a una creciente implementación de las tecnologías de la información y las comunicaciones en diversos ámbitos del sector salud. Tal implementación ha incrementado el volumen de datos personales de la salud que son tratados en los sistemas de información que los almacenan. Sin embargo, la baja calidad o la falta de integración entre los sistemas de información son algunos de los factores que limitan alcanzar los beneficios esperados con el tratamiento de los datos de la salud.

De acuerdo con la OCDE, el anterior contexto refleja que las sociedades no están acostumbradas a generar información para lograr los objetivos de los sistemas de salud. Así mismo, reconoce que los desarrollos tecnológicos que permiten tratar los datos personales de salud también introducen nuevos riesgos para la protección de la privacidad y la seguridad de los datos.

Mediante su Recomendación sobre gobernanza de los datos de salud del año 2017, la OCDE promueve ver los datos como un recurso fundamental de los sistemas de salud, sociedades y de la comunidad global. A su vez, promueve llegar a un consenso internacional sobre las condiciones que deben regir el tratamiento de los datos de salud, incorporando un enfoque que proteja los intereses públicos atendidos por estos recursos, y que permita maximizar los beneficios y disminuir los riesgos del tratamiento.

En atención a que la Recomendación OCDE es considerada como referente para la implementación efectiva de los servicios digitales de salud, y teniendo en cuenta los crecientes esfuerzos por digitalizar el tratamiento de los datos del sistema de salud colombiano junto con los nuevos riesgos que ello implica, este artículo de investigación pretende responder a la pregunta sobre si la protección dada a los datos tratados por el sistema de salud colombiano, resulta acorde con lo previsto por la Recomendación OCDE sobre gobernanza de los datos de salud.

Para responder a la pregunta planteada, se siguió un programa de investigación que inicia con la descripción de la protección en Colombia respecto al tratamiento de datos personales relacionados con la salud. Luego, se describe lo propuesto en la Recomendación OCDE sobre gobernanza de los datos de la salud, y finalmente se contrastan algunos datos relacionados con el contexto colombiano frente a dicha recomendación.

El programa de investigación tuvo un enfoque de tipo documental y el método empleado es de tipo cualitativo deductivo. Se abordó la identificación, análisis y síntesis de la información relevante para responder al problema planteado, acudiendo principalmente a recursos de investigación digitales, entre ellos, Dialnet, Google Scholar, Hein Online, Jstor, OECD/OCDE iLibrary, Redalyc, SCIELO, Science Direct, Taylor & Francis, así

como a los sistemas de información del Estado colombiano como SUIN-Juriscol y los buscadores tradicionales de jurisprudencia y doctrina.

La pregunta planteada no pretende responderse mediante un análisis exhaustivo, pues el objetivo consiste en identificar algunas situaciones relacionadas con el tratamiento del dato de la salud en Colombia, así como describir la recomendación OCDE sobre gobernanza de los datos de la salud, para finalmente perfilar el caso colombiano mediante algunos datos interpretados en función al contenido de dicha Recomendación.

1. TRATAMIENTO DEL DATO DE LA SALUD Y SU NIVEL DE PROTECCIÓN EN COLOMBIA

INTRODUCCIÓN

En este capítulo se aborda el nivel de protección dado al tratamiento del dato de la salud en la Colombia, partiendo de la aproximación al sistema de salud colombiano, en orden a identificar algunos de los distintos tipos de datos que caracterizan el funcionamiento del sector salud. También se abordará la legislación aplicable al tratamiento de los datos personales, así como los desafíos del sistema de salud frente al tratamiento de datos personales. Por último, se hace una breve referencia a los ajustes que necesita el sector salud.

1.1.APROXIMACIÓN AL SISTEMA DE SALUD COLOMBIANO

El servicio público de salud es prestado desde el año 1993 en el marco del Sistema General de Seguridad Social, conformado por los regímenes generales establecidos para pensiones, salud, riesgos laborales y los servicios sociales complementarios¹.

El sistema de salud es definido como “el conjunto articulado y armónico de principios y normas; políticas públicas; instituciones; competencias y procedimientos; facultades, obligaciones, derechos y deberes; financiamiento; controles; información y evaluación, que el Estado disponga para la garantía y materialización del derecho fundamental de la salud”².

El ordenamiento jurídico colombiano inicialmente reconoció la salud como garantía fundamental por conexidad, esto es, por su relación directa con otros derechos fundamentales, tales como la vida y la integridad física. En otro momento, el reconocimiento de la salud como derecho fundamental derivó de ciertas condiciones atribuibles al titular del derecho, como fue por ejemplo el caso de los adultos mayores. Y desde el año 2007, la Corte Constitucional calificó como “artificioso” acudir a la conexidad

¹ L. 100/1991, art. 8.

² L.1751/2015, art. 4.

para reconocer el carácter fundamental del derecho a la salud, siendo desde entonces innecesario aludir a la conexidad con otros derechos para considerarlo fundamental³.

Con la expedición de la Ley estatutaria 1751 de 2015, iniciativa de los profesionales de la salud y que fue radicada por el Gobierno Nacional⁴, el derecho a la salud adquirió carácter fundamental, autónomo e irrenunciable en lo individual y en lo colectivo. En la materialización de este derecho interactúan varios tipos de participantes, entre ellos los usuarios del sistema, los agentes reguladores (Ministerio de Salud y protección Social - Minsalud- y Ministerio de Hacienda y Crédito Público -Minhacienda-), los sujetos regulados y vigilados (aseguradores y prestadores de servicios⁵), la Superintendencia Nacional de Salud -Supersalud-, como encargada de la inspección, vigilancia y control, otras entidades de control, representantes de gremio y expertos⁶.

El derecho a la salud comprende el acceso a los servicios de salud de manera oportuna, eficaz y con calidad para la preservación, el mejoramiento y la promoción de la salud⁷. Igualmente, se orienta por principios como el de la universalidad del aseguramiento y de la prestación de los servicios del plan de beneficios a todos los residentes del país, en todas sus etapas de la vida⁸. Lo anterior, en el marco del modelo de aseguramiento realizado mediante el régimen contributivo o subsidiado⁹, siendo obligatoria la afiliación al sistema para todos los habitantes en Colombia, a quienes se les garantiza el acceso a los servicios independientemente de su capacidad de pago¹⁰.

A su vez, el derecho a la salud incluye elementos esenciales e interrelacionados en materia de disponibilidad, aceptabilidad, calidad e idoneidad profesional, y accesibilidad¹¹. La disponibilidad es entendida como el deber a cargo del Estado, de garantizar la existencia de servicios y tecnologías e instituciones de salud, así como de programas de salud y personal médico y profesional competente¹².

³ C. Constitucional., Sent. C-313, may. 29/2014. M.P. Gabriel Eduardo Mendoza Martelo.

⁴ Defensoría del Pueblo de Colombia. La tutela y los derechos a la salud y a la seguridad social. 13 ed., Bogotá, 2019. p. 84

⁵ GALLOR LINARES, Luisa Manuela; HERNÁNDEZ MONROY, Daniela Alexandra; NIETO VANEGAS, Jineth Alejandra. Explicación y análisis del Sistema de Seguridad Social en Salud en Colombia. [en línea]. En: Revista Digital Isocuenta, 2017 vol. 2, no. 11. [Citado en el 01 de junio de 2019]. p. 12. Disponible en: <https://revistas.usantotomas.edu.co/index.php/isocuenta/article/view/4330>

⁶ SUÁREZ ROZO, Luisa Fernanda, *et. al.* La crisis del sistema de salud colombiano: una aproximación desde la legitimidad y la regulación. [en línea]. En: Rev Gerenc Polít Salud, 2017, vol. 16, no 32. [Citado en el 18 de junio de 2019]. p. 39. Disponible en: <http://dx.doi.org/10.11144/javeriana.rgps16-32.cssc>

⁷ L.1751/2015, art. 2.

⁸ L. 1751/2015, art. 6, literal a.

⁹ L. 100/1993, art. 157.

¹⁰ L. 100/1993, art. 153, numeral 1.

¹¹ L.1751/2015, art. 6.

¹² L. 1751/2015, art. 6, literal a.

En virtud de la calidad e idoneidad profesional, los establecimientos, servicios y tecnologías de salud requieren personal de la salud competente¹³. La aceptabilidad se orienta a que los agentes del sistema sean respetuosos de la ética médica, así como de las diversas culturas de las personas, minorías étnicas, pueblos y comunidades, respetando sus particularidades socioculturales y cosmovisión de la salud, permitiendo su participación en las decisiones del sistema de salud que le afecten¹⁴.

La participación en el sector se proyecta en diversos escenarios, que incluyen la formulación de la política de salud, los planes para su implementación; las instancias de deliberación, veeduría y seguimiento del Sistema; los programas de promoción y prevención; decisiones de inclusión o exclusión de servicios y tecnologías; los procesos de definición de prioridades de salud; las decisiones que puedan significar una limitación o restricción en las condiciones de acceso a establecimientos de salud; la evaluación de los resultados de las políticas de salud¹⁵.

En cuanto a la accesibilidad, este elemento del derecho a la salud consiste en que los servicios y tecnologías deben ser accesibles a todos, en condiciones de igualdad, dentro del respeto a las especificidades de los diversos grupos vulnerables y al pluralismo cultural. Este elemento comprende la no discriminación, la accesibilidad física, la asequibilidad económica y el acceso a la información¹⁶.

A pesar del reconocimiento normativo del derecho fundamental a la salud en Colombia, en el año 2018 se interpusieron 207.734 acciones de tutela, correspondientes al 34,21 por ciento del total de las acciones interpuestas en el país, donde los accionantes invocaron el derecho fundamental a la salud de manera individualizada o en conjunto con otros derechos. Tales cifras representan un incremento del 5,1 por ciento con relación al año 2017, e indican que cada 2,5 minutos se interpone una tutela en salud, o cada 34 segundos si se tiene en cuenta solo los 246 días hábiles de 2018, siendo la cifra más alta desde el establecimiento de la acción de tutela con la Constitución Política de 1991¹⁷.

Antioquia, Valle del Cauca y Bogotá son las regiones con más acciones interpuestas para exigir el derecho a la salud a través de este mecanismo, factor que puede atribuirse a “la facilidad de acceso a la justicia, a la oferta importante de servicios de salud de alta tecnología, así como a la densidad de población y al nivel cultural”¹⁸. Con los anteriores datos, fue posible para la Defensoría del Pueblo inferir que las acciones de tutela interpuestas son directamente proporcionales al conocimiento que los usuarios tienen de sus derechos, igualmente proporcional al acceso a los servicios judiciales.

¹³ L. 1751/2015, art. 6, literal d

¹⁴ L. 1751/2015, art. 6, literal b

¹⁵ L. 1751/2015, art. 12

¹⁶ L. 1751/2015, art. 6, literal b.

¹⁷ DEFENSORÍA DEL PUEBLO DE COLOMBIA. Op. cit., p. 84-85

¹⁸ *Ibíd.*, p. 89

Ahora bien, el aumento en las cifras genera interrogantes sobre las verdaderas razones del incremento en la cantidad de acciones interpuestas, las cuales podrían relacionarse con la suficiencia de las medidas adoptadas por el Gobierno Nacional y el Minsalud para la garantía efectiva del derecho a la salud en los elementos de accesibilidad, calidad, disponibilidad y aceptabilidad, la reglamentación y aplicación de las normas, o el incremento en el nivel de exigencia por parte de los usuarios¹⁹.

Debido a factores como el volumen de casos abordados por la jurisprudencia, las bases de datos del sistema de seguridad social, entre ellas, las relacionadas con la salud, son “quizás las bases de datos más importantes para el Estado Social de Derecho, por la interdependencia creciente que significan para el goce efectivo de un haz de derechos fundamentales de un gran número de personas”²⁰.

La información sobre la salud de las personas no se restringe únicamente a la historia clínica²¹, considerada “el único archivo o banco de datos donde legítimamente reposan, todas las evaluaciones, pruebas, intervenciones y diagnósticos realizados al paciente”²². Los datos de la salud en Colombia pueden estar contenidos en diferentes sistemas de información cuya definición, diseño, reglamentación, implantación y administración de aquellos que operan dentro del sistema de salud corresponde al Minsalud en participación con las entidades territoriales²³.

A continuación, se presentan aspectos clave para caracterizar algunos de los soportes de datos de la salud existentes en el sistema de salud colombiano:

1.1.1. Bases de datos de la salud. Colombia actualmente cuenta con sistemas que tratan datos de la salud que, de acuerdo con la OCDE, han introducido innovaciones interesantes al momento de planificar la entrega de valor público a la sociedad²⁴. A continuación, se hace referencia al Sistema de Información Integral de la Protección Social (SISPRO) y al Sistema de afiliación transaccional (SAT), los cuales le han permitido al Minsalud pasar de tener sistemas verticales con los que brindaba servicios individualmente considerados, a contar con soluciones transversales que prestan servicios integrados.

1.1.1.1. SISPRO. Este sistema de información²⁵ actualmente se estructura como una bodega de datos que contiene aquellos gestionados por el Minsalud²⁶, considerados como

¹⁹ *Ibíd.*, p. 86.

²⁰ UPEGUI MEJÍA, Juan Carlos. *Habeas Data: Fundamentos, naturaleza, régimen*. Bogotá: Universidad Externado de Colombia. 2008. p. 291.

²¹ *Ibíd.*, p. 292.

²² Sentencia T-275 de 2005, citado por: UPEGUI MEJÍA, Juan Carlos. *Op. cit.*, p. 193.

²³ L. 715/ 2001, art. 42.

²⁴ OCDE. *Gobernanza de la transformación digital del sector público colombiano*. En: *Revisión del Gobierno Digital en Colombia: Hacia un Sector Público Impulsado por el Ciudadano*, París, 2018. [Citado en el 3 de noviembre de 2019]. p. 41-42. Disponible en: <https://doi.org/10.1787/9789264292147-4-es>

²⁵ L. 1438/2011, art. 112.

necesarios para la construcción de indicadores y reportes. Sus fuentes de información tienen una estructura de reporte y consolidación independiente, que provienen de fuentes internas y externas al Minsalud²⁷.

De acuerdo con el catálogo de información del Minsalud, con fecha de corte a septiembre 30 de 2019²⁸, se pueden identificar las siguientes características del SISPRO:

- La información que allí se almacena, está relacionada con alguno de los siguientes componentes estratégicos del sistema de salud y protección social: Aseguramiento; financiamiento; oferta; demanda y uso y; vigilancia y control.
- Las temáticas usadas para organizar la información dentro de cada componente estratégico son las siguientes: Población, afiliación e identificación de la población, financiamiento, prestación de servicios de salud, estado de salud, factores de riesgo, participación social, instituciones, mercado de servicios de salud, planeación y regulación²⁹.
- La información es solicitada en virtud de fuentes normativas de diversos rangos (ley, decreto, resolución, circular, circular conjunta, nota externa), de carácter nacional, departamental o municipal, las cuales pueden establecer o no la definición de las variables a solicitar a través de anexos técnicos.
- Las entidades obligadas a reportar pueden enviar al Minsalud la información mediante los siguientes mecanismos: PISIS (plataforma de integración de datos del SISPRO), aplicativo web, CD, correo electrónico, correo certificado.
- Actualmente existen noventa y siete fuentes de información que, en función al componente estratégico, pueden ser las siguientes:
 - Aseguramiento: Cuenta con dieciocho fuentes, entre ellas, el Registro Único de Afiliados a la Protección Social (RUAF), y la base de datos única de afiliados (BDUA);
 - Demanda y uso: Cuenta con veinticuatro fuentes, entre ellas, el Registro Individual de prestación de servicios en salud (RIPS), el Registro Único de Afiliados – Módulo de Nacimientos y Defunciones (RUAF-ND), el Registro de Actividades de Protección Específica y Detección Temprana, el Programa Ampliado de Inmunizaciones Web (PAIWEB); la verificación de la entrega de la carta de derechos y deberes del afiliado y del paciente y de la carta de desempeño de la EPS.

²⁶ L. 1122/2007, art. 44.

²⁷ ORDUÑA ORTEGÓN, Yeimi Pilar. Avances en la construcción de un sistema de información en salud en Colombia. [en línea]. En: Cienc Tecnol Salud Vis Ocul, 2014, vol. 12, no. 2. [Citado en el 2 de noviembre de 2019]. p. 82. Disponible en: <https://doi.org/10.19052/sv.3297>

²⁸ Catálogo de información del Ministerio de Salud y Protección Social. [Consultado en el 27 de octubre de 2019]. Disponible en: <https://www.sispro.gov.co/catalogos/Pages/catalogo-de-informacion.aspx>

²⁹ Res. 2542/1998, MINSALUD, art. 3, parágrafo 1.

- **Financiamiento:** Cuenta con treinta y tres fuentes, entre ellas: el reporte de facturas, recobros, reclamaciones y novedades de pago relacionadas con la prestación de servicios de salud y las facturas pagadas por giro directo a IPS de acuerdo con el monto certificado por las EPS-S; el Reporte de prescripción, suministro, verificación, y análisis de la información de tecnologías en salud no financiadas con recursos de la UPC y servicios complementarios (MipresNoPBS); Los proceso de verificación, control y pago de las solicitudes de recobro de medicamentos, procedimientos y otras atenciones en salud.
- **Oferta:** Cuenta con trece fuentes, entre ellas el Registro Especial de Prestadores de Servicios de Salud (REPS); el Sistema de Información Hospitalaria (SIHO); el Registro Único Nacional del Talento Humano en Salud (RETHUS); el Sistema de Información de Medicamentos (SISMED); El Sistema de Vigilancia en Salud Pública (SIVIGILA); El Sistema de Información de la Vigilancia de la Calidad del Agua para Consumo Humano (SIVICAP); Servicio Social Obligatorio.
- **Vigilancia y Control:** Cuenta con nueve fuentes, entre ellas el Sistema de Información para la Calidad; Listados censales de las poblaciones especiales; Relaciones entre prestadores de servicios de salud y entidades responsables del pago de servicios de salud.

Mediante SISPRO, el Minsalud integra las fuentes de información usadas por el Sistema de Registros, Observatorios y Sistemas de Seguimiento Nacionales (ROSS)³⁰, el cual tiene capacidad de monitorear la trayectoria de salud de individuos, población y los determinantes socioeconómicos³¹. Las fuentes de información del sistema ROSS son los registros administrativos, encuestas y estudios poblacionales, y censos de población especial³², las cuales están integradas en los términos y condiciones de oportunidad, cobertura y calidad según los estándares de transferencia determinados por el Minsalud³³.

La implementación del sistema ROSS busca facilitar la generación de información relevante, nuevas soluciones en investigación y la gestión del conocimiento, así como corregir fallas de regulación o de inspección y vigilancia. Para ello, debe operar en línea entre los diferentes agentes del sistema, generar reportes, alertas y datos suficientes en tiempo real, y permitir que los usuarios y las autoridades obtengan oportunamente el

³⁰ Res. 1281/2014, MINSALUD.

³¹ MINSALUD. Guía Metodológica para Registros, Observatorios, Sistemas de Seguimiento y Salas Situacionales Nacionales en Salud ROSS. Bogotá, 2015. [Citado en el 3 de mayo de 2019]. p. 97. Disponible en:

https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VS/ED/GCFI/ROSS_001.11.2013.pdf

³² Ibid., p. 47.

³³ Res. 1281/2014, MINSALUD, art. 3.

conocimiento del sector, siendo obligatorio el suministro de información veraz e imparcial³⁴.

Según los Término de Uso del SISPRO, la información personal tratada en razón al suministro de datos hecho por el usuario mediante los formularios de contacto incluye: nombre, edad, género, dirección, correo y electrónico. Ahora bien, esta política no describe cuáles son los datos personales que trata en función a sus diversas fuentes de información, tampoco se refiere a aspectos tales como los derechos de los titulares de los datos, o a la finalidad del tratamiento³⁵.

1.1.1.2. SAT. Es el sistema de información creado por el Minsalud para agrupar, unificar y simplificar las reglas de afiliación al Sistema General de Seguridad Social en Salud (SGSSS), a fin de reducir los trámites requeridos y eliminar las barreras que afectan el acceso a los servicios de salud de los afiliados³⁶.

El SAT permite registrar y consultar, en tiempo real, los datos de información básica y complementaria de los afiliados, la afiliación y sus novedades en los Sistemas Generales de Seguridad Social en Salud y en Riesgos Laborales³⁷, mediante la página web www.miseguridadsocial.gov.co. Dentro de los datos personales que pueden ser suministrados por el usuario en su registro se incluyen los siguientes: nombre, identificación, edad, sexo, dirección, correo electrónico y teléfono³⁸.

Con el SAT, el Minsalud busca centralizar y facilitar al usuario la gestión de sus servicios de seguridad social, en cuanto a su afiliación, reporte de novedades, consulta de la planilla de pago de aportes al SGSSS y la validación de información administrativa de pensión, caja de compensación familiar, riesgos laborales y salud relacionada con EPS, SISBEN o grupo familiar. Los datos personales son tratados por el SAT para finalidades como: “(i) la adecuada gestión y administración de los servicios ofrecidos en el sitio web, en los que el usuario decida utilizar o darse de alta; (ii) el estudio cuantitativo y cualitativo de las visitas y de la utilización de los servicios por parte de los usuarios; (iii) el envío por medios

³⁴ C. Constitucional., Sent. C-313, may. 29/2014. M.P. Gabriel Eduardo Mendoza Martelo.

³⁵ MINSALUD. Políticas de Uso y Privacidad del Portal WEB SISPRO. [en línea]. Consultado en el 03 de noviembre de 2019. p. 1. Disponible en: https://www.minsalud.gov.co/Documents/Ministerio/Terminos%20y%20Condiciones%20de%20uso%20del%20portal%20web_Octubre%202012x.pdf

³⁶ D. 2353/2015, MINSALUD, considerando.

³⁷ D. 780/2016, MINSALUD, art. 2.1.2.1 anterior D. 2353/2015, art. 11.

³⁸ Términos y condiciones de uso de Mi Seguridad Social. [en línea]. Consultado en el 03 de noviembre de 2019. p. 3. Disponible en: <https://miseguridadsocial.gov.co/Registro/ValidacionDatosBasicos/DownloadFileTerminosCondiciones?Length=4>

tradicionales y electrónicos de información relacionados con el Ministerio y de cualquier otro proyecto del Ministerio, sus funciones y las de las entidades adscritas y vinculadas”³⁹.

1.1.2. La historia clínica. Es el registro obligatorio, cronológico, claro, preciso, completo, expreso, legible de las condiciones de salud del paciente⁴⁰, de tipo somático, psíquico, social, cultural, económico y medioambiental que pueden incidir en su salud⁴¹. En razón a ello, la historia clínica es considerada como el documento más importante de toda la relación médico-paciente, pues contiene la información producida en el marco de dicha relación, compuesta por datos personales de carácter reservado, calificados como sensibles⁴².

1.1.2.1. Contenido. La historia clínica contiene todo el cuadro clínico en las distintas fases del acto médico. Los datos allí registrados abarcan los antecedentes, la anamnesis, el diagnóstico, tratamiento, medicamentos aplicados, la evolución, el seguimiento, control, protocolo quirúrgico, indicación del equipo médico, registro de la anestesia, los estudios complementarios, la ubicación en el centro hospitalario, el personal de la salud involucrado en la atención, las pruebas diagnósticas, etc.⁴³

La información contenida en la historia clínica es parte fundamental de la práctica médica, al ser el registro histórico de la atención dada a un individuo, indispensable para una atención integral. Por ello, es una actividad sujeta a principios y estándares profesionales actualmente regulados en las normas sobre ética médica⁴⁴.

Así mismo, en la historia clínica se documenta el consentimiento informado dado por el paciente que recibe determinada atención en salud. Dicho consentimiento es uno de los fundamentos de cada una de las etapas en la relación clínica, y consiste en el proceso permanente de comunicación entre el equipo de salud y el paciente, el cual responde a una exigencia ética y legal que busca defender la dignidad y los derechos de los pacientes⁴⁵.

1.1.2.2. Usos. La historia clínica le pertenece a la persona y la institución que presta el servicio de salud cumple un deber de custodia y cuidado⁴⁶. Puede usarse como material de consulta y apoyo a los trabajos médicos, siguiendo los principios del secreto profesional, de

³⁹ *Ibíd.*, p. 4.

⁴⁰ L. 23/1981, art. 34.

⁴¹ Res. 1995/1999., MINSALUD.

⁴² CORREA MARTÍNEZ, César. La historia clínica. Aspectos jurídicos y dilemas en el derecho español y colombiano. [en línea]. En: *VieI*, 2015, vol. 10, no. 2 [citado en el 7 de mayo de 2019]. p. 130. Disponible en: <https://doi.org/10.15332/s1909-0528.2015.0002.03>

⁴³ CSJ, Cas. Civil, Sent. Dic. 14/2018, Rad. 5641. M.P. Margarita Cabello Blanco

⁴⁴ L. 23/1981.

⁴⁵ ESCOBAR LÓPEZ, María Teresa; NOVOA TORRES, Edgar. Análisis de formatos de consentimiento informado en Colombia. [en línea]. En: *Revista Latinoamericana de Bioética*, 2016, vol. 30, no. 1. [Citado el 22 de julio de 2019]. p. 19. Disponible en: <https://doi.org/10.18359/r/bi.1439>

⁴⁶ DUR. 780/2016, art. 2.8.1.5.4.

la propiedad intelectual, y la ley estatutaria de protección de datos personales⁴⁷. También sirve a la labor de auditoría adelantada por las entidades administradoras de recursos del Sistema General de Seguridad Social, tales como EPS, ARL, etc.⁴⁸

La historia clínica es muy utilizada como fuente de datos para fines investigativos. En Colombia, las investigaciones en salud se clasifican según el riesgo que representan para los participantes⁴⁹. La investigación donde se apliquen técnicas de revisión documental retrospectiva, revisión de historias clínicas, entrevistas, cuestionarios y otros, corresponde a la categoría de investigaciones sin riesgo⁵⁰.

1.1.2.3. Conservación. Todos los prestadores de servicios de salud deben tener el archivo único de historias clínicas, organizado según los principios generales definidos por el Archivo General de la Nación⁵¹, quienes pueden utilizar programas automatizados para diligenciar y manejar las historias clínicas⁵². Los equipos y soportes documentales deben contar con mecanismos de seguridad para impedir que la historia clínica sea modificada, en forma accidental o provocada, una vez se registren los datos⁵³.

Cada historia clínica debe conservarse mínimo por quince años, contados a partir de la fecha de la última atención. Ese periodo se duplicará cuando los datos correspondan a víctimas de violaciones de derechos humanos o infracciones graves al Derecho Internacional Humanitario, y si se trata de una historia clínica que forme parte de un proceso relacionado con delitos de lesa humanidad, la conservación será permanente⁵⁴.

1.1.2.4. Carácter reservado. La historia clínica es un documento privado sometido a reserva, que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley, debiendo en todo caso mantenerse la reserva legal. Los sujetos autorizados normativamente para acceder son: a) El usuario; b) El Equipo de Salud; c) Las autoridades judiciales y de salud en los casos previstos en la Ley; d) Las demás personas determinadas en la ley⁵⁵. Tal autorización debe contener de forma expresa e inequívoca la manifestación de la voluntad del paciente y/o usuario, para que determinada persona pueda tener acceso a la misma, y no se ha contemplado ningún formalismo para tal fin⁵⁶.

⁴⁷ DUR. 780/2016, art. 2.7.2.2.1.1.25; Res. 839/2017, art. 11.

⁴⁸ DUR. 780/2016, art. 2.5.3.4.11

⁴⁹ Res. 8430/1993, art. 11, MINSALUD.

⁵⁰ MATEUS, Julio Cesar, *et al.* Resolución 8430 de 1993: ¿Responde a las necesidades actuales de la ética en investigación en salud con seres humanos en Colombia? [en línea]. En: Biomédica, 2019, vol. 39, no. 3. [Citado en el 8 de julio de 2019]. p. 16. Disponible en:

<https://www.revistabiomedica.org/index.php/biomedica/article/view/4333>

⁵¹ R. 1995/1999, art. 12. MINSALUD.

⁵² R. 1995/1999, art. 18. MINSALUD

⁵³ R. 1995/1999, art. 18. MINSALUD

⁵⁴ R. 839/2017, art. 3. MINSALUD

⁵⁵ R. 1995/1999, art. 1. literal a. MINSALUD

⁵⁶ Concepto 201811600757601/2018. MINSALUD

El carácter reservado de la historia clínica obedece a la mayor protección requerida, pues la divulgación de los datos de la salud en el ámbito social puede dar lugar a conductas discriminatorias, que potencialmente pueden causar perjuicios a su titular por ejemplo en mercados como el laboral o el de seguros⁵⁷.

Dentro de las normas del sector salud que se refieren a la reserva de la historia clínica se destaca la Ley estatutaria de la salud, según la cual las personas tienen derecho a que sea tratada de manera confidencial y reservada, así como también tienen derecho a consultar la totalidad de su historia clínica en forma gratuita, a obtener copia de esta, y a que únicamente pueda ser conocida por terceros, previa autorización del paciente o en los casos previstos en la ley⁵⁸. Igualmente, la Ley de ética médica cataloga a la historia clínica como un documento privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley⁵⁹.

A su vez, el Código de Procedimiento Administrativo y de lo Contencioso Administrativo dispone que solo tendrán carácter reservado las informaciones y documentos expresamente sometidos a reserva por la Constitución Política o la ley, y en especial, los que involucren derechos a la privacidad e intimidad de las personas, haciendo referencia expresa a la historia clínica⁶⁰. También dispone que la solicitud de información contenida en la historia clínica, por ser de carácter reservado, solo pueda ser solicitada por el titular de la información, por sus apoderados o por personas autorizadas con facultad expresa para acceder a esa información⁶¹.

1.1.2.5. Historia clínica electrónica. La historia clínica es una importante fuente de datos que facilita la comunicación entre diversos agentes del sistema de salud. Su potencial para generar información relevante del sector salud es tal, que a nivel internacional se promueve la implementación de la Historia Clínica Electrónica (HCE)⁶², para que brinde información completa y accesible sobre cada paciente en el punto donde es atendido, a fin de mejorar la

⁵⁷ TRAVIESO Juan Antonio. La protección de datos personales: salud e investigación clínica médica. En: TRAVIESO Juan Antonio (Comp.). Régimen jurídico de los datos personales. Argentina: Abeledo Perrot, 2014 (Tomo II), p. 920.

⁵⁸ L. 1751/2015, art.10, literal g.

⁵⁹ L. 23/1981, art. 34.

⁶⁰ L.1755/2015, art. 24 y 27.

⁶¹ L.1755/2015, art. 24, parágrafo.

⁶² OPS. Registros médicos electrónicos en América Latina y el Caribe: Análisis sobre la situación actual y recomendaciones para la Región. [en línea]. Washington, 2016. [Citado en el 3 de mayo de 2019]. p. 9. Disponible en:
<http://www.paho.org/relacsis/index.php/biblioteca-usuarios/biblioteca-de-publicaciones/item/572-publicacion-registros-medicos-electronicos-en-america-latina-y-el-caribe>

calidad y oportunidad de la atención en salud, así como proporcionar mejores datos sobre la efectividad y la cobertura de las intervenciones⁶³.

Según la OMS, la HCE es un importante componente para lograr la cobertura universal de salud. Si bien su implementación puede ser compleja y costosa, tiene el potencial de promover la atención de calidad, la reducción de costos, el apoyo a la movilidad del paciente, el aumento de la confiabilidad de la información, y acceso a la información para múltiples proveedores de atención en salud. Lo anterior, sin exponer al usuario a dificultades financieras⁶⁴.

Colombia es uno de los países miembro de la OMS que aún no cuenta con HCE⁶⁵, y cada vez que una persona se traslada de un prestador de servicios de salud a otro, se genera una nueva historia clínica, lo que representa una pérdida de información sobre condiciones de salud ya registradas⁶⁶.

Ahora bien, con la expedición del Plan Nacional de Desarrollo 2015-2018, la HCE fue incluida en los Servicios Ciudadanos Digitales⁶⁷, definidos estos como “el conjunto de servicios que brindan capacidades y eficiencias para optimizar y facilitar el adecuado acceso de los usuarios a la administración pública a través de medios electrónicos”⁶⁸. Estos servicios apuntan a transformar los servicios de datos de las entidades públicas, modificando así la relación entre la ciudadanía y el Estado⁶⁹.

En Colombia le corresponde al Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con las entidades responsables de cada uno de los trámites y servicios, definir y expedir los estándares, modelos, lineamientos y normas

⁶³ OMS. Global diffusion of eHealth: making universal health coverage achievable. Report of the third global survey on eHealth. [en línea]. 2016. [Citado en el 3 de mayo de 2019]. p. 6. Disponible en: https://www.who.int/goe/publications/global_diffusion/en/ [Traducido por la autora]

⁶⁴ OMS. Electronic health records. En: Global diffusion of eHealth: making universal health coverage achievable. Report of the third global survey on eHealth. Ginebra, 2016. [Citado en el 3 de mayo de 2019]. p. 94. Disponible en: https://www.who.int/goe/publications/global_diffusion/en/ [Traducido por la autora]

⁶⁵ OMS. Perfil de Colombia en el uso de *eHealth* [en línea]. En: Atlas of eHealth country profiles 2015: The use of eHealth in support of universal health coverage Based on the findings of the 2015 global survey on eHealth. 2016. [Citado en el 3 de mayo de 2019]. p. 2. Disponible en: https://www.who.int/goe/publications/atlas_2015/en/ [Traducido por la autora]

⁶⁶ RENDÓN GUTIÉRREZ, Iván Santiago, *et al.* Historias clínicas digitales desde la perspectiva colombiana: seguridad, calidad y gestión del dato. [en línea]. En: *Inventum*, 2018, vol. 13, no. 24. [Citado en el 3 de mayo de 2019]. p. 25. Disponible en: <https://doi.org/10.26620/uniminuto.inventum.13.24.2018.22-28>

⁶⁷ L.1753/2015, art. 45.

⁶⁸ DUR 1078/2015, art. 2.2.17.1.3., numeral 19, adicionado por D. 1413/2017, art. 1.

⁶⁹ LÓPEZ, Joan. Servicios ciudadanos digitales e historias clínicas electrónicas. [en línea]. Bogotá, 2019. [Citado en el 17 de mayo de 2019]. p. 8. Disponible en: <https://karisma.org.co/otrashistorias/documentation/scd-hce/>

técnicas para la incorporación de las TIC aplicables a los servicios ciudadanos digitales, incluida la HCE⁷⁰.

1.2. DESAFÍOS DEL SISTEMA DE SALUD FRENTE AL TRATAMIENTO DE DATOS PERSONALES

Incrementar el uso de las TIC en los sistemas de salud es considerado como una estrategia para avanzar hacia una mejor atención de las personas, aumentando la eficiencia del sistema en su conjunto y proporcionando la base para futuras innovaciones en la atención en salud. En punto al tratamiento de datos, se afirma que las TIC conducen a mejorar el cuidado de cada paciente, permitiendo manejar los registros médicos de manera integrada, lo cual aumenta las posibilidades de acceder a los servicios de salud⁷¹, así como también ayudan a prevenir errores médicos evitables⁷² y a suministrar medicina personalizada, dada la posibilidad de analizar grandes volúmenes de datos que permitan hacer diagnósticos predictivos y sugerir tratamientos para los pacientes⁷³.

Con la expedición del Plan Nacional de Desarrollo 2015-2018 y la inclusión de la historia clínica electrónica en los Servicios Ciudadanos Digitales, podría considerarse que Colombia está avanzando hacia esa mejor atención asociada a la implementación de las TIC en el tratamiento de los datos del sistema de salud. Sin embargo, organizaciones de la sociedad civil han alertado sobre cómo el modelo proyectado por el Gobierno transforma los datos de la historia clínica, “en activos que serán administrados por privados y que pueden ser explotados para otros propósitos, mientras los aleja[n] de su verdadera función: prestar el servicio de salud”, y ello tendría lugar a pesar de la falta de participación de todos los actores del sector salud en dicha transformación⁷⁴.

Tal alerta invita a reflexionar sobre los desafíos del sistema de salud frente al tratamiento de datos personales puesto que, para avanzar hacia una mejor atención en salud, se requiere proteger los derechos de los titulares de los datos. Lo anterior implica, entre otros asuntos, usar los datos para la finalidad que dio lugar a su entrega. Igualmente, se requiere permitir a las organizaciones maximizar el uso inteligente de la información, aumentando su nivel de competitividad y consolidando una buena reputación empresarial o institucional, mediante

⁷⁰ L. 1753/2015, art. 45.

⁷¹ RUBÍ NAVARRETE, Jesús. En: TRAVIESO, Juan Antonio (Comp.). Régimen jurídico de los datos personales. Argentina: Abeledo Perrot, 2014 (Tomo II), p. 938.

⁷² PRICE, William Nicholson. Risk and Resilience in Health Data Infrastructure. [en línea]. En: Colo. Tech. L.J., 2017, vol. 16. no. 1. [Citado en el 8 de mayo de 2019]. p. 66. Disponible en: <http://dx.doi.org/10.2139/ssrn.2928997> [Traducido por la autora]

⁷³ CRAWFORD, Kate, SCHULTZ Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. [en línea]. En: Boston College Law Review, 2014, vol. 55, no. 93 [Citado en el 8 de mayo de 2019]. p.102. Disponible en: <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4> [Traducido por la autora]

⁷⁴ BOTERO CABRERA, Carolina. Las historias de los Servicios Ciudadanos Digitales. En: El espectador. Bogotá, 27 de Julio de 2019. Disponible en: <https://www.elspectador.com/opinion/las-historias-de-los-servicios-ciudadanos-digitales-columna-873130>

la implementación de medidas proactivas de protección⁷⁵, que les permitan ser transparentes con los titulares de los datos al tiempo que generan confianza en el mercado⁷⁶.

En ese sentido, resulta relevante identificar el estado actual de la legislación aplicable al tratamiento de datos, para luego abordar los desafíos del régimen de protección de datos dada la creciente digitalización de aquellos que son tratados en el sistema de salud colombiano, en orden a identificar los ajustes que necesita el sector.

1.2.1. Legislación aplicable al tratamiento de los datos personales. En Colombia, la protección de los datos personales es un derecho constitucional y fundamental, en virtud del cual se exige el respeto por la libertad y demás garantías constitucionales en la recolección, tratamiento y circulación de los datos personales, junto con el cumplimiento de unos mínimos con independencia del sistema de información que contenga los datos tratados⁷⁷.

El tratamiento de datos se refiere a cualquier operación o conjunto de operaciones sobre datos personales, con o sin ayuda de la informática, sometido a ciertos principios jurídicos que buscan impedir el uso abusivo y arbitrario de la facultad informática⁷⁸.

Este derecho protege a las personas cuando sus datos son recolectados, almacenados y utilizados por terceros. También confiere una serie de derechos para que los titulares de los datos sean sujetos activos, hasta donde puedan, de lo que sucede con sus datos personales⁷⁹.

Las principales reglas aplicables al tratamiento de datos personales están contenidas en la Constitución Política de 1991⁸⁰, la Ley Estatutaria 1581 de 2012, el Decreto 1377 de 2013, y la jurisprudencia de la Corte Constitucional. La creación de la Ley 1581 obedeció, entre otras razones, a la necesidad de generar un marco legal para que Colombia contara con el nivel adecuado de protección frente a las autoridades europeas, y que fuese competitivo

⁷⁵ REMOLINA ANGARITA, Nelson; ÁLVAREZ ZULUAGA, Luisa Fernanda. Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability– en las transferencias internacionales de datos personales. [en línea]. Bogotá, Universidad de los Andes, 2018. [Citado en el 8 de mayo de 2019]. p. 7. Disponible en: <https://habeasdatacolombia.uniandes.edu.co/?p=2817>

⁷⁶ SIC. Guía para la implementación del principio de responsabilidad demostrada (Accountability). [en línea] Bogotá, 2015, [Citado en el 10 de mayo de 2019]. p. 24. Disponible en: <http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>

⁷⁷ REMOLINA ANGARITA, Nelson. Tratamiento de datos personales relativos a la salud: reflexiones en torno a la incidencia de la Ley 1581 de 2012 en el sector salud. Bogotá: Universidad de los Andes, 2014, p. 4.

⁷⁸ C. Constitucional., Sent. C -748, oct. 06/2011. M.P. Jorge Ignacio Pretelt Chaljub. Numeral 2.4.3.2.

⁷⁹ REMOLINA ANGARITA, Nelson. Realidades y reflexiones sobre el tratamiento de datos personales en Latinoamérica. En: TRAVIESO, Juan Antonio (Comp.). Régimen jurídico de los datos personales. Argentina: Abeledo Perrot, 2014 (Tomo II), p.1083.

⁸⁰ C.N., art. 15.

para facilitar la realización de negocios relacionados con el tratamiento de datos personales⁸¹.

Para la Ley 1581 de 2012, cualquier operación realizada sobre datos personales determina la aplicación de sus reglas, independientemente de si el tratamiento se relaciona con una base de datos personales, debido a que su propósito es regular “todas las operaciones y conjunto de operaciones con los datos personales”⁸². Es también una ley estatutaria neutral desde una perspectiva tecnológica porque aplica transversalmente a toda actividad que involucre datos personales mediante cualquier tipo de tecnología actual o futura⁸³.

El alcance de dicha ley abarca las bases de datos públicas y privadas, así como cualquier tratamiento de datos personales que tenga lugar en Colombia y el realizado por personas ubicadas fuera del país en territorios bajo jurisdicción colombiana de acuerdo con los estándares y tratados internacionales. La Ley 1581 también aclaró los conceptos relacionados con los datos personales, y calificó el consentimiento que los titulares deben dar a los responsables para que estos recopilen sus datos y lleven a cabo el tratamiento⁸⁴.

Los responsables del tratamiento son quienes garantizan las condiciones de confidencialidad y de seguridad para impedir cualquier tratamiento ilícito⁸⁵. A su vez son tenedores, por ende, no son dueños de los datos personales contenidos en sus bases de datos o archivos. En consecuencia, deben administrar la información de las personas de manera correcta, apropiada y acertada porque su negligencia o dolo afecta los derechos humanos de los titulares de los datos⁸⁶. Así mismo, deben observar los principios aplicables al tratamiento de datos personales, a fin de poder considerar que el tratamiento es constitucionalmente legítimo.

El contenido mínimo del derecho a la protección de datos se relaciona con los siguientes derechos: Conocer las bases de datos que contienen información recogida sobre las personas; incluir nuevos datos que den una imagen completa del titular; actualizar la información; rectificar o corregir la información para que concuerde con la realidad; excluir información bien por el uso indebido o por simple voluntad del titular, salvo excepciones

⁸¹ REMOLINA ANGARITA, Nelson. Recolección internacional de datos personales: un reto del mundo post-internet. Madrid: BOE. 2015. p. 136.

⁸² UPEGUI MEJÍA, Juan Carlos. Comentario a la sentencia T-020 de 2014 de la Corte Constitucional colombiana. Apuntes sobre el “tratamiento estructurado de datos personales”. [en línea]. En: Estudios en Derecho a la Información, 2017, no. 4. [Citado en el 10 de noviembre de 2019]. p. 96-97. Disponible en: <https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/11522/13407>

⁸³ Cir. Ext. 04/2019, SIC, ANDJE.

⁸⁴ OSMÁ PERALTA, Sarah. 2018. The Role of search engines in Colombia after the Muebles Caqueta vs. Google Inc decision. [en línea]. En: Revista La Propiedad Inmaterial, 2018, no. 26. [Citado en el 10 de noviembre de 2019]. p. 148. Disponible en: <https://doi.org/10.18601/16571959.n26.06> [Traducido por la autora]

⁸⁵ C. Constitucional., Sent. C -748, oct. 06/2011. M.P. Jorge Ignacio Pretelt Chaljub. Numeral 2.5.7.3.

⁸⁶ Res. 83882/2018, SIC.

normativas⁸⁷; autorizar la inclusión de la información recaudada en una base datos, en ejercicio de los derechos a la autodeterminación informática y el principio de libertad⁸⁸.

En punto a los datos de la salud, el marco jurídico de protección de datos los ubica en una categoría especial de datos personales. Ese tratamiento particular deriva de la complejidad de las cuestiones científicas que giran alrededor de la salud de las personas, o a que los datos pueden referirse a un individuo, a su núcleo familiar o un grupo de personas, por ejemplo, los datos genéticos⁸⁹.

El dato de la salud no se encuentra definido normativamente en Colombia. Ahora bien, la ley estatutaria sobre protección de datos personales dispone que los datos relativos a la salud corresponden a la categoría de datos sensibles que afectan la intimidad del Titular o un uso indebido puede generar su discriminación⁹⁰. Son datos categorizados internacionalmente como sensibles porque un tratamiento indebido afecta derechos y libertades de las personas⁹¹.

Si bien no existe reglamentación de la ley estatutaria sobre protección de datos personales que sea específica y completa respecto de los datos de salud⁹², las normas preexistentes a dicha ley que sean aplicables al tratamiento de datos relativos a la salud, las historias clínicas y demás relacionadas con el tratamiento de datos personales, deben ser observadas, aplicadas, complementadas e interpretadas por los sujetos involucrados en la recolección y uso de esa información, de manera conjunta y armónica con la Ley estatutaria sobre protección de datos⁹³.

Al ser un dato sensible, el tratamiento de datos de la salud se encuentra en principio prohibido, y excepcionalmente pueden ser tratados⁹⁴, por ejemplo, cuando el titular haya dado autorización explícita para ello, o cuando se trate de datos relacionados con la salud que resulten necesarios para la adecuada prestación del servicio médico y permitan salvaguardar un interés vital del titular y este se encuentre física o jurídicamente incapacitado⁹⁵.

⁸⁷ C. Constitucional., Sent. C -748, oct. 06/2011. M.P. Jorge Ignacio Pretelt Chaljub. Numeral 2.1.1.2.

⁸⁸ REMOLINA ANGARITA, Nelson. Tratamiento de datos personales relativos a la salud: reflexiones en torno a la incidencia de la Ley 1581 de 2012 en el sector salud. Op. cit., p. 4.

⁸⁹ REMOLINA ANGARITA, Nelson. Tratamiento de datos personales relativos a la salud: reflexiones en torno a la incidencia de la Ley 1581 de 2012 en el sector salud. Op. cit., p. 7.

⁹⁰ L.1581/2012, art. 5.

⁹¹ REMOLINA ANGARITA, Nelson. Tratamiento de datos personales relativos a la salud: reflexiones en torno a la incidencia de la Ley 1581 de 2012 en el sector salud. Op. cit., p. 7.

⁹² CORREA MARTÍNEZ. César. Op. cit., p. 133.

⁹³ REMOLINA ANGARITA, Nelson. Tratamiento de datos personales relativos a la salud: reflexiones en torno a la incidencia de la Ley 1581 de 2012 en el sector salud. Op. cit., p. 7-8.

⁹⁴ L.1581/2012, art. 6.

⁹⁵ Concepto 17644871/2017. SIC

El responsable del tratamiento debe solicitar al titular la autorización para el tratamiento de los datos, a más tardar en el momento de su recolección y según los procedimientos que adopte para ello. También debe informarle los datos personales que serán recolectados, así como todas las finalidades específicas del tratamiento para las cuales se obtiene el consentimiento⁹⁶.

Igualmente, en el tratamiento de datos sensibles se deberá: i. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su tratamiento; ii. Informar al titular, de forma explícita y previa, los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento, así como obtener su consentimiento expreso. Y ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles⁹⁷.

El responsable del tratamiento debe adoptar mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado, que garanticen su consulta. Esos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada⁹⁸. Para el caso de los datos sensibles, la autorización explícita se refiere solo a que sea escrita o verbal⁹⁹.

Ahora bien, el tratamiento sin autorización del titular se permite: i) Cuando sea necesario para salvaguardar el interés vital del titular y éste se encuentre física o jurídicamente incapacitado, caso en donde los representantes legales deberán otorgar su autorización; ii) Si se trata de una urgencia médica o sanitaria¹⁰⁰, donde no sea posible obtener la autorización del titular o resulte particularmente problemático gestionarla, dadas las circunstancias de apremio, riesgo o peligro para otros derechos fundamentales, ya sea del titular o de terceras personas; iii) Cuando exista un expreso mandato legal o judicial que releve el consentimiento previo del titular cuando ha establecido la obligatoriedad de un determinado tratamiento de datos personales para la prestación del servicio de salud¹⁰¹.

El debido tratamiento de datos personales en sistemas de información interoperables está protegido por los principios transversales reconocidos en la Ley 1581 de 2012, los cuales que deben ser aplicados en cualquier actividad sin importar la novedad de las operaciones que se están realizando o las tecnologías utilizadas para dicho efecto. Por tal motivo, la Superintendencia de Industria y Comercio, en calidad de autoridad nacional de protección de datos personales, considera que en Colombia no existe un vacío legislativo frente al

⁹⁶ DUR.1074/2015. art. 2.2.2.25.2.2.

⁹⁷ DUR.1074/2015. art. 2.2.2.25.2.3.

⁹⁸ DUR.1074/2015. art. 2.2.2.25.4.1.

⁹⁹ Concepto 17644871/2017. SIC

¹⁰⁰ L. 1581/2012, art. 10, literal c.

¹⁰¹ C. Constitucional., Sent. C -748, oct. 06/2011. M.P. Jorge Ignacio Pretelt Chaljub. Numeral 2.12.3.

tratamiento de información personal en sectores donde no existe una legislación específica o respecto del surgimiento de nuevas tecnologías o fenómenos tecnológicos¹⁰².

1.2.2. Desafíos del sector salud. El sistema de salud colombiano presenta un desequilibrio entre los agentes del sistema de salud respecto del conocimiento de la información tratada en este sector. Lo anterior ha generado una ventaja informativa para los encargados de materializar el derecho a la salud, junto con barreras administrativas principalmente asumidas por los usuarios, traducidas en limitantes para acceder a los servicios de salud¹⁰³.

Tales asimetrías de información entre los participantes del sistema obedecen a que los encargados del aseguramiento y la prestación efectiva de los servicios tienen, en razón a su objeto social, un acceso cotidiano a la información. En contraste, los usuarios carecen de esta a pesar de que, por ejemplo, el Minsalud debe establecer indicadores para que los usuarios cuenten con información objetiva del sistema de salud, a fin de reducir las asimetrías de información y garantizar su derecho a la libre elección de los prestadores de servicios y aseguradores¹⁰⁴.

A su vez, los datos reportados por determinados agentes del sistema de salud colombiano¹⁰⁵, son recibidos por sistemas de información considerados débiles y desarticulados¹⁰⁶. La información tratada en esos sistemas se presenta como bodegas de datos aisladas, sin mecanismos que faciliten su interoperabilidad y funcionalidad para seguir los procesos y resultados de los servicios de salud, a fin de garantizar su acceso, uso y calidad¹⁰⁷.

Esa falta de integración duplica los esfuerzos para generar reportes, así como también disminuye la calidad de la información¹⁰⁸. Adicionalmente, explica situaciones como el escaso reconocimiento social de las funciones de inspección, vigilancia y control entre los

¹⁰² Cir. Ext. 04/2019, SIC, ANDJE.

¹⁰³ ÁLVAREZ SALAZAR, Gabriel Jaime, GARCÍA GALLEGÓ, Marilyn, LONDOÑO USME, Maritza. Crisis de la salud en Colombia: limitantes del acceso al derecho fundamental a la salud de los adultos mayores. [en línea]. En: Revista CES Derecho, 2016, vol. 7, no. 2. [Citado en el 3 de mayo de 2019]. p. 117-118. Disponible en: <http://dx.doi.org/10.21615/cesder.7.2.8>

¹⁰⁴ L.1438/2011, art.108.

¹⁰⁵ BERNAL ACEVEDO, Oscar, FORERO CAMACHO, Juan Camilo. Sistemas de información en el sector salud en Colombia. [en línea]. En: Revista Gerencia y políticas de salud, 2011, vol. 10, no. 21. [Citado en el 3 de mayo de 2019]. p. 89-90. Disponible en: <https://revistas.javeriana.edu.co/index.php/gerepolsal/article/view/2590>

¹⁰⁶ SUÁREZ ROZO, Luisa Fernanda, *et. al.* Op. cit., p. 43.

¹⁰⁷ ESLAVA RINCÓN, Julia, *et al.* 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. [en línea]. En: Revista Gerencia y políticas de salud, 2018, vol. 17, no 35. [Citado en el 3 de mayo de 2019]. p. 9. Disponible en: <https://doi.org/10.11144/Javeriana.rgps17-35.acrs>

¹⁰⁸ BERNAL ACEVEDO, Oscar, FORERO CAMACHO, Juan Camilo. Op. cit., p. 89.

usuarios del sistema de salud colombiano¹⁰⁹, e incide en que la vigilancia de los agentes se base en información desactualizada¹¹⁰.

En el Plan Nacional de Desarrollo 2018-2022 se dispone que el Minsalud adoptará un mecanismo electrónico para desarrollar la interoperabilidad de la historia clínica, el cual “deberá garantizar que todos los prestadores de servicios de salud públicos y privados, y demás personas naturales o jurídicas que se relacionen con la atención en salud, compartan los datos vitales definidos por el Gobierno nacional para dar continuidad a la atención en salud, los cuales deberán cumplir los estándares que se establezcan para el efecto”¹¹¹.

El Minsalud reconoce que el desarrollo de una historia clínica electrónica única o de la interoperabilidad de la historia clínica, no garantizan por sí mismo el acceso y ejercicio del derecho a la salud¹¹². Ahora bien, los Servicios Ciudadanos Digitales, junto con otros componentes y habilitadores transversales definidos en la Política de gobierno digital para Colombia, “permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC”¹¹³.

Como parte de los servicios ciudadanos digitales, se desarrolla una carpeta ciudadana para archivar y consultar documentos clave para las interacciones de los ciudadanos con el Estado. Su confiabilidad y seguridad se apoya en un sistema de autenticación electrónico y biométrico y un modelo de interoperabilidad para el intercambio de datos e integración de sistemas entre instituciones públicas¹¹⁴.

La interoperabilidad es entendida como la habilidad de dos o más sistemas para intercambiar información y hacer uso de los datos intercambiados, siendo necesario que además del intercambio, se entienda la información intercambiada¹¹⁵. Normativamente, la interoperabilidad se define como la “aptitud de los sistemas y aplicaciones, basados en tecnologías de la información y las comunicaciones, y los procesos que estos soportan, para intercambiar información y posibilitar utilizar mutuamente la información intercambiada”¹¹⁶.

¹⁰⁹ ESLAVA RINCÓN, Julia, *et al.* Op. cit., p. 10

¹¹⁰ SUÁREZ ROZO, Luisa Fernanda, *et. al.* Op. cit., p. 43.

¹¹¹ L. 1955/2019, art. 246

¹¹² Concepto jurídico del Ministerio de Salud y Protección Social al Proyecto de Ley número 233 de 2019. Senado. Gaceta del Congreso 403. 2019. p. 10

¹¹³ D. 1078/2015, art. 2.2.9.1.2.1.

¹¹⁴ OCDE. El contexto del gobierno digital en Colombia. En: Evaluación de Impacto del Gobierno Digital en Colombia: Hacia una Nueva Metodología, Paris, 2017a. [Citado en el 3 de mayo de 2019]. p. 28. Disponible en: <https://doi.org/10.1787/9789264284272-3-es>

¹¹⁵ LÓPEZ SEVILLANO, Alexandra María, SALCEDO PARRA, Octavio José, REYES DAZA, Brayan. Análisis del estado actual de la salud pública bajo el marco de la interoperabilidad. [en línea]. En: Revista científica Puente, 2015. vol. 9, no. 2. [Citado en el 3 de mayo de 2019]. p. 9. Disponible en: <https://revistas.upb.edu.co/index.php/puente/article/view/7104>

¹¹⁶ Res. 202/2010, MINTIC, art. 1.

Los servicios de interoperabilidad son definidos como aquellos que brindan las capacidades necesarias para garantizar el adecuado flujo de información y de interacción entre los sistemas de información de las entidades del Estado, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales”¹¹⁷.

De acuerdo con los lineamientos definidos por la Superintendencia de industria y Comercio (SIC) y la Agencia Nacional de Defensa Jurídica del Estado (ANDJE), la interoperabilidad entre sistemas de información donde circulan datos personales debe realizarse conforme a los principios señalados en la Ley 1581 de 2012, por lo que no es necesaria la expedición de una norma adicional y específica para este fin¹¹⁸.

Con la reglamentación de los servicios ciudadanos digitales se creó el Articulador, “entidad encargada de adelantar las interacciones con los distintos actores involucrados en la prestación de los servicios ciudadanos digitales para lograr una prestación coordinada y adecuada de tales servicios”¹¹⁹. Esta entidad público-privada define las condiciones del sistema, educa a la ciudadanía, otorga concesiones a las empresas operadoras del sistema, y vigila y controla al Operador¹²⁰, que es la persona jurídica prestadora de los servicios ciudadanos digitales¹²¹. En el año 2018, la Corporación Agencia Nacional Digital (AND) fue creada como la entidad encargada de articular los servicios ciudadanos digitales¹²².

1.2.3. Ajustes que necesita el sector salud. Podría considerarse que, con la inclusión de la historia clínica electrónica en los Servicios Ciudadanos Digitales, las ineficiencias en la prestación del servicio de salud podrán ser abordadas a fin de superar las barreras administrativas que limitan a los usuarios acceder a los servicios de salud.

Los sistemas interconectados potencialmente ofrecen un gran valor, pero también pueden conllevar mayores riesgos de seguridad, que concretados pueden amenazar la confianza y desalentar la disposición para compartir datos¹²³. Adicionalmente, la implementación de las TIC puede resultar compleja¹²⁴, el suministro de medicina personalizada requerirá del acceso a datos de la salud muy detallados sobre un individuo, así como a miles de otros perfiles que permitan comparar las predicciones generadas. Entonces, los tratamientos

¹¹⁷ DUR. 1078/2015, art.2.2.17.2.1.1, núm. 1.5, adicionado por D. 1413/2017, art. 1.

¹¹⁸ Cir. Ext. 04/2019, SIC, ANDJE.

¹¹⁹ DUR. 1078/2015, art. 2.2.17.1.3. núm. 2, adicionado por D. 1413/2017, art. 1.

¹²⁰ LÓPEZ, Joan. Op. cit. p. 7

¹²¹ DUR. 1078/2015, art. 2.2.17.1.3. núm. 16. adicionado por D. 1413/2017, art. 1.

¹²² D. 2257/2017, art. 1.

¹²³ PRONOVOST, Peter, *et. al.* 2018. Procuring Interoperability: Achieving High-Quality, Connected, and Person-Centered Care. [en línea]. Washington: National Academy of Medicine. [Citado en el 3 de mayo de 2019]. p. 97. Disponible en: <https://nam.edu/procuring-interoperability-achieving-high-quality-connected-and-person-centered-care/> [Traducido por la autora]

¹²⁴ OPS. Op. cit., p. 17.

médicos sugeridos podrían estar asociados al individuo de la misma manera que si se tratase de información de carácter personal¹²⁵.

Dicho contexto implica acumular una mayor cantidad de datos del sector salud, lo cual crea nuevos riesgos relacionados con la privacidad y protección de datos sensibles. A su vez, surge un mayor interés por parte de terceros para acceder a tal información¹²⁶, y pueden producirse daños por la inclusión inapropiada de los datos personales y el análisis predictivo sin el conocimiento o consentimiento expreso del titular¹²⁷.

Así mismo, el uso de historias clínicas electrónicas se encuentra expuesto a la pérdida de datos o el registro de datos incorrectos; la presentación de datos para el paciente equivocado; el caos durante la inactividad del sistema; la no disponibilidad del sistema para su uso¹²⁸. Incluso, la falta de implementación de políticas internas efectivas para garantizar la seguridad de los datos puede llevar a la sanción del responsable de tratamiento en caso de que estos sean vulnerados, por ejemplo, por su exposición masiva en internet¹²⁹.

Según fueron concebidos los Servicios Ciudadanos Digitales, es posible que estos generen valor público en el sistema de salud colombiano, particularmente ayudando a superar las asimetrías de información entre agentes del sistema y las ineficiencias en la prestación del servicio de salud. Ahora bien, aún no es clara la forma que va a tomar la historia clínica electrónica en Colombia¹³⁰, así como tampoco es claro cómo se articulará el operador de servicios ciudadanos digitales con el sistema de salud, sus elementos y principios, y los datos que allí se tratan.

Por lo tanto, es necesario que el Gobierno promueva y haga efectiva la participación de todas las partes interesadas, especialmente de los usuarios del sistema de salud, para así evitar que los problemas del Sistema de Salud en Colombia se profundicen y terminen alejando a las personas de la garantía de sus derechos¹³¹. Así mismo, cobra relevancia la identificación del espectro de riesgos que implica tratar los datos¹³², así como la real y debida implementación de principios como el de responsabilidad demostrada (*accountability*).

¹²⁵ CRAWFORD, Kate, SCHULTZ Jason. Op. cit., p. 102.

¹²⁶ RUBÍ NAVARRETE, Jesús. Op. cit., p. 938.

¹²⁷ CRAWFORD, Kate, SCHULTZ Jason. Op. cit., p. 94.

¹²⁸ MINSALUD Interoperabilidad para una propuesta de un sistema de Historia Electrónica de Salud. [en línea]. Bogotá, 2013. [Citado en el 16 de junio de 2019]. p. 60. Disponible en: <https://consultorsalud.com/wp-content/uploads/2014/10/interoperabilidad-proyecto-esalud.pdf>

¹²⁹ R. 61062/2018. SIC.

¹³⁰ BOTERO CABRERA, Carolina. Op. Cit.

¹³¹ CASTAÑEDA, Juan Diego. ¿Otra vez la misma historia? Cuando las TIC se interponen entre la ciudadanía y el Estado. Disponible en: <https://karisma.org.co/otrashistorias/documentation/otra-vez/>

¹³² RAYMOND, Anjanette. Information and the Regulatory Landscape: A Growing Need to Reconsider Existing Legal Frameworks. [en línea]. En: Wash. & Lee J. Civ. Rts. & Soc. Just, 2018, vol. 24, no. 357. [Citado en el 08 de mayo de 2019]. p. 378. Disponible en: <https://dx.doi.org/10.2139/ssrn.3349737>

Y para lograrlo, es necesario que los operadores de servicios ciudadanos digitales adopten medidas apropiadas, efectivas y verificables que les permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales; Creen e implementen un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales; El PIGD debe cumplir con las instrucciones de la Superintendencia de Industria y Comercio, en particular, la guía para la implementación del principio de responsabilidad demostrada (accountability) de dicha entidad¹³³.

CONCLUSIONES

- El marco jurídico colombiano protege la salud como un derecho fundamental, donde el acceso a los servicios de salud debe ser oportuno, eficaz y con calidad. Sin embargo, la cantidad de acciones de tutela interpuestas en el año 2018 para exigir el derecho a la salud a través de este mecanismo, junto con el incremento en tales cifras, podría relacionarse con la insuficiencia de las medidas adoptadas por el Gobierno Nacional y el Minsalud para la garantía efectiva del derecho a la salud en los elementos de accesibilidad, calidad, disponibilidad y aceptabilidad, así como a debilidades en la reglamentación y aplicación de las normas, y al incremento en el nivel de exigencia por parte de los usuarios.
- Los agentes del sector salud generan datos almacenados en varios sistemas de información que cumplen diversos fines. Estos sistemas son débiles y desarticulados, debido a factores como la falta de integración entre ellos o la baja calidad de la información. Lo anterior genera una ventaja informativa para los encargados de materializar el derecho a la salud, junto con barreras administrativas asumidas principalmente por los usuarios. A su vez, contribuyen al desequilibrio entre agentes respecto del conocimiento de la información de la salud, y a las ineficiencias en la prestación del servicio de salud.
- En razón a que la historia clínica tiene potencial para generar información relevante del sector salud, actualmente se promueve la implementación de la Historia Clínica Electrónica en el marco de los Servicios Ciudadanos Digitales. Ahora bien, aún no es clara la forma que va a tomar la historia clínica electrónica en Colombia, y la participación de todas las partes interesadas no está ocurriendo, aspecto que preocupa porque la implementación de la HCE genera una mayor acumulación de datos en el sector salud, crea nuevos riesgos relacionados con la privacidad y protección de datos sensibles, y surge un mayor interés por parte de terceros para acceder a tal información.

¹³³ D. 1078/2015, art. 2.2.17.6.3., adicionado por D. 1413/2017, art. 1.

2. TRATAMIENTO DEL DATO DE LA SALUD Y SU NIVEL DE PROTECCIÓN SEGÚN EL ESTÁNDAR OCDE

INTRODUCCIÓN

En este capítulo se aborda el nivel de protección dado al tratamiento del dato de la salud en la OCDE, partiendo de la descripción sobre la importancia de los datos en los sistemas de salud, así como de los riesgos y factores clave para que la información genere valor. También se abordarán algunos aspectos relacionados con la implementación de la historia clínica electrónica en países miembro de la OCDE. Por último, se hace referencia al marco recomendado por la OCDE para la gobernanza de los datos personales de la salud, los mecanismos clave para maximizar beneficios y disminuir riesgos, así como a la aplicación del marco OCDE a Colombia.

2.1. LOS DATOS DE LA SALUD SEGÚN LA OCDE

La OCDE considera que los sistemas públicos y privados de atención en salud pertenecen a la industria de la información y el conocimiento. Estos sistemas generan grandes cantidades de datos, dentro y fuera de los límites convencionales del sistema de salud, y de varios tipos: clínicos, diagnósticos, administrativos, financieros, genéticos, demográficos, comportamentales y medioambientales¹³⁴.

La OCDE también promueve que la medicina se concentre en prevenir la aparición de enfermedades y controlar su avance, mejorar la calidad y coordinación de la atención en salud, encontrar nuevas formas para lograr sistemas más productivos y sostenibles. Para ello, los sistemas de salud tienden hacia un mayor uso de datos clínicos y administrativos, a fin de evaluar la efectividad de las terapias y servicios¹³⁵.

Sin embargo, el crecimiento de los sistemas de salud en su tamaño y complejidad, así como el cambio de las necesidades de la población, dada su evolución clínica y cultural, no se ha armonizado con la evolución en la estructura de los sistemas de salud y su gobernanza. Estos sistemas están quedándose atrás de otras industrias en el aprovechamiento de los datos, lo que puede deberse a que las sociedades no están acostumbradas a generar información valiosa para lograr los objetivos de los sistemas de salud¹³⁶.

Por ejemplo, la atención de salud invierte menos del 5% de sus ingresos en los sistemas de información, inversión que es inferior al 1% en países de bajos y medianos ingresos, una cantidad insignificante para pertenecer al sector de la información, en comparación con el

¹³⁴ OCDE. Digital technology: Making better use of health data. En: *New Health Technologies: Managing Access, Value and Sustainability*. Paris, 2017b. [Citado en el 15 de mayo de 2019]. p. 187. Disponible en: <https://doi.org/10.1787/9789264266438-9-en>. [Traducido por la autora]

¹³⁵ OCDE. Introducing high-value, privacy-protective health information systems. En: OCDE. *Health Data Governance: Privacy, Monitoring and Research*. Paris, 2015a. [Citado en el 3 de mayo de 2019]. p. 20. Disponible en: <https://doi.org/10.1787/9789264244566-5-en>. [Traducido por la autora]

¹³⁶ *Ibíd.*, p. 195.

13% que dedica la industria bancaria en esos sistemas¹³⁷. La generación de datos de la salud produce poca información, pues muchas veces son datos desordenados y desestructurados. Y los problemas para proporcionar información correcta, en el momento adecuado a determinada persona o actor (pacientes, cuidadores, proveedores o administradores), derivan en fallas en la atención en salud¹³⁸.

El tratamiento de datos de la salud se enfrenta a problemas clave relacionados con la falta de claridad en cómo poner en práctica la legislación sobre protección de los datos. Lo anterior se refiere a aspectos como el consentimiento informado, la legalidad de compartir datos entre autoridades públicas, y el acceso a datos personales de la salud para investigación. Adicionalmente, los instrumentos legislativos que gobiernan los datos, privacidad y seguridad son previos a la era digital, lo que hace necesario actualizar los mecanismos legales que permiten el uso de datos de la salud¹³⁹. Entonces, resulta importante abordar los problemas clave relacionados con el tratamiento de datos personales de salud, dados los importantes riesgos que representa para la privacidad de las personas, y para los individuos y sociedades.

Los daños que podrían resultar del mal uso de los datos de la salud, por una parte, pueden incluir: a) daños financieros, reflejados en discriminación en el aseguramiento de la salud o el empleo; b) psicosociales, como vergüenza, estigma y pérdida de reputación, lo que resulta en aislamiento y estrés; c) pérdida de la confianza pública en el gobierno y sus instituciones, incluida la pérdida de confianza en el sistema de atención médica¹⁴⁰.

Por otra parte, existe el riesgo de que las sociedades pierdan la oportunidad de monitorear e informar sobre la salud de su población y la calidad y seguridad de los servicios de atención médica. También se eleva el riesgo a que las personas experimenten una atención médica ineficiente, ineficaz e incluso perjudicial. Y la sociedad puede perder la oportunidad de investigar e innovar para mejorar la salud y los resultados de la atención médica¹⁴¹.

Para que los datos de la salud generen cualquier valor, deben ser combinados, armonizados, manejados y analizados. Esto requiere invertir en infraestructura técnica y en capital humano, así como adoptar las leyes requeridas. Igualmente, los sistemas de salud necesitan desarrollar un marco de gobernanza que articule todos los aspectos técnicos, legales y recursos para el manejo de datos. Ahora bien, para que el marco de gobernanza refleje

¹³⁷ OMS, OCDE, Banco Mundial. Delivering Quality Health Services: A Global Imperative for universal health coverage. [en línea]. Ginebra, 2018. [Citado en el 20 de mayo de 2019]. p. 18. Disponible en: <https://doi.org/10.1787/9789264300309-en> [Traducido por la autora]

¹³⁸ OCDE. 2017b. Op. cit., p. 190

¹³⁹ OCDE. 2017b. Op. cit., p. 199

¹⁴⁰ OCDE. Protection of privacy in the collection and use of personal health data. En: Strengthening Health Information Infrastructure for Health Care Quality Governance. [en línea]. Paris, 2013a. [Citado en el 11 de mayo de 2019]. p. 88. Disponible en: <https://doi.org/10.1787/9789264193505-9-en> [Traducido por la autora]

¹⁴¹ *Ibíd.*, p. 88.

valores y prioridades sociales, los gobiernos necesitan de canales claros y abiertos para involucrarse con las partes interesadas en el desarrollo y uso de los datos¹⁴².

Entonces, cobra importancia asegurar que la información relevante sobre determinado individuo llegue a las personas adecuadas en el momento adecuado, pues ello permite una toma de decisiones más precisa, oportuna y coordinada en todos los entornos de atención. Y de acuerdo con la OCDE, sólo las técnicas analíticas basadas en *big data* son capaces de acceder y procesar los diversos tipos de datos para permitir que la información se genere de manera oportuna¹⁴³.

2.2. LA HISTORIA CLÍNICA ELECTRÓNICA EN PAÍSES OCDE

El uso de datos de salud se habilita en gran medida por el acceso a una Historia Clínica Electrónica (HCE) integrada. La información que de allí se obtiene permite lograr objetivos clave en materia de salud pública, desempeño del sistema de salud, vigilancia de la seguridad del paciente, investigación para avanzar en la salud de la población y la atención de la salud. También aporta datos a los ensayos clínicos, y permite a los médicos consultar datos para informar sus decisiones sobre el tratamiento de pacientes individuales¹⁴⁴.

El uso de la HCE en consultorios médicos y hospitales es alto en muchos países de la OCDE. Sin embargo, un problema común a todos ellos, incluso donde la implementación de la HCE ha tenido un buen progreso, se relaciona con la posibilidad de compartir los registros electrónicos entre los médicos de atención primaria y los especialistas¹⁴⁵.

En cuanto a los requisitos sobre la estructura de los datos y los estándares de contenido, la OCDE ha encontrado que estos varían entre países. Lo anterior es relevante porque los datos estructurados, al ser comparables, se pueden extraer fácilmente para usos de monitoreo e investigación. Los datos no estructurados comprenden texto de flujo libre y son difíciles de analizar¹⁴⁶.

Dentro de los factores clave que permiten contar con datos estructurados, se encuentran: a) Una organización nacional responsable de establecer la terminología clínica nacional y los estándares de mensajería electrónica; b) Todos o la mayoría de los registros de salud electrónicos tienen codificados datos clave como diagnóstico, medicamentos, pruebas de laboratorio, imágenes médicas, procedimientos quirúrgicos, según una norma de terminología clínica; c) Existen instrumentos de política (legislación, certificaciones, incentivos financieros) para exigir o alentar a los proveedores de atención médica a adoptar un sistema de registro electrónico que cumpla con la terminología clínica nacional y los

¹⁴² Ibíd., p. 194.

¹⁴³ Ibíd., p. 190-191.

¹⁴⁴ OCDE. 2017b. Op. cit., p. 205

¹⁴⁵ OCDE. 2017b. Op. cit., p. 208.

¹⁴⁶ OCDE. 2017b. Op. cit., p. 209.

estándares de mensajería electrónica, lo cual permite compartir los registros entre los proveedores de atención médica¹⁴⁷.

La OCDE también ha identificado que casi todos los países utilizan identificadores únicos nacionales para pacientes y proveedores de atención médica, a fin de respaldar los controles de calidad de los datos y facilitar el enlace de los datos de la HCE con otros conjuntos de datos¹⁴⁸.

En cuanto a los desafíos relacionados con la calidad de los datos y sus soluciones, estos también se abordan de manera diferente en cada país. Dentro de las soluciones se encontraron: el establecimiento de terminología nacional y estándares de interoperabilidad; la creación de un conjunto de datos mínimos de carácter nacional y estandarizado; el uso de instrumentos de política para alentar o exigir a los proveedores de atención médica que adopten y utilicen sistemas de HCE que cumplan con los requisitos nacionales; la auditoria al contenido de la HCE¹⁴⁹.

La OCDE promueve que los países cuenten con un marco regulatorio adecuado, que incentive la innovación para generar buenos diseños, con adecuada funcionalidad, y que puedan enlazarse con otras fuentes de información. Y gracias a la experiencia de los países miembro que han progresado en la implementación de la HCE, construyó indicadores clave para identificar la preparación de un país en cuanto a la gestión datos mediante la HCE.

Dichos indicadores son los siguientes¹⁵⁰: 1) Tener un marco jurídico que permita extraer datos dentro de las HCE con fines estadísticos y de investigación, sujeto a las garantías adecuadas; 2) Tener un plan o política nacional de HCE que incluya los usos estadísticos y de investigación de estos datos; 3) Participar en la extracción de datos de la HCE para crear conjuntos de datos nacionales; 4) Analizar los datos extraídos de la HCE en función a los objetivos nacionales clave de monitoreo e investigación, y para invertir en el desarrollo de información de salud.

Aunque la preparación para gestionar datos de la HCE es baja en muchos países, la OCDE identificó que la mayoría están implementando un sistema nacional de HCE. Los países que han progresado en su implementación ofrecen ejemplos clave en materia de gobernanza, y aquellos con la mayor capacidad técnica y operativa están en mejor posición para desarrollar información nacional de salud a partir de los datos contenidos en la HCE¹⁵¹.

¹⁴⁷ OCDE. 2017b. Op. cit., p. 210.

¹⁴⁸ OCDE. 2017b. Op. cit., p. 210.

¹⁴⁹ OCDE. 2017b. Op. cit., p. 212.

¹⁵⁰ OCDE. 2017b. Op. cit., p. 205

¹⁵¹ OCDE. 2017b. Op. cit., p. 204

2.3. MARCO OCDE PARA LA GOBERNANZA DE LOS DATOS PERSONALES DE LA SALUD

La OCDE ha insistido en la necesidad de llegar a un consenso internacional sobre las condiciones que deben regir el tratamiento de los datos de la salud, tanto a nivel nacional como transnacional, incorporando un enfoque gubernamental completo. Lo mencionado obedece a los intereses públicos atendidos por esa información, que abarcan los ámbitos de la salud, la justicia, la industria, la ciencia, la innovación y las finanzas¹⁵².

Por ello, en el año 2017 la OCDE presentó su recomendación relacionada con la gobernanza de los datos de la salud. Allí afirmó que para maximizar los beneficios sociales y minimizar los riesgos sociales derivados del uso del dato de la salud, se requiere desarrollar una fuerte gobernanza enmarcada normativamente para soportar un tratamiento que proteja la privacidad de dichos datos.

Así mismo, identificó las condiciones y mecanismos clave para maximizar beneficios y disminuir riesgos, en donde las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, y los principios allí contenidos, establecen las condiciones para lograr una mayor armonización de los marcos de gobernanza de los datos, permitiendo que estos sean usados para investigación, estadísticas y mejora de la calidad de la atención de salud¹⁵³.

La Recomendación del Consejo de la OCDE sobre Gobernanza de los Datos de Salud es una de las múltiples declaraciones de políticas sobre el acceso y el intercambio de datos de la salud, creados a nivel de entidades gubernamentales, la industria, agencias regulatorias e instituciones públicas y privadas¹⁵⁴. Ese tipo de declaraciones reflejan que la gobernanza en materia de protección de datos, consentimiento, ética y acceso a los datos resulta ser mucho más exigente en el sector salud que en cualquier otro sector¹⁵⁵.

La recomendación de la OCDE es considerada legalmente como no vinculante, a menudo denominada como *soft law*. Su contenido aplica al acceso y al procesamiento de datos

¹⁵² OCDE. Recommendation of the OECD Council on Health Data Governance. [en línea]. Paris, Health Ministerial Meeting, 2017c. [Citado en el 10 de mayo de 2019]. p. 12. Disponible en: <http://www.oecd.org/health/ministerial/ministerial-statement-2017.pdf> [Traducido por la autora]

¹⁵³ *Ibíd.*, p. 1.

¹⁵⁴ KALKMAN, Shona, *et al.* Responsible data sharing in international health research: a systematic review of principles and norms. [en línea]. En: BMC Med Ethics, 2019, vol. 20, no. 21. [Citado en el 20 de mayo de 2019]. p. 9-11. Disponible en: <https://doi.org/10.1186/s12910-019-0359-9> [Traducido por la autora]

¹⁵⁵ EICHLER, Hans-Georg, *et al.* Hans-Georg, *et al.* Data Rich, Information Poor: Can We Use Electronic Health Records to Create a Learning Healthcare System for Pharmaceuticals? [en línea]. En: Clinical Pharmacology & Therapeutics, 2018, vol. 105, no. 4. [Citado en el 23 de mayo de 2019]. P. 917. Disponible en: <https://doi.org/10.1002/cpt.1226> [Traducido por la autora]

personales de salud para fines de interés público relacionados con la salud¹⁵⁶, y se dirigen tanto a los gobiernos como a las instituciones no gubernamentales¹⁵⁷.

Puede que la Recomendación sea poco conocida, pero su debate público podría ser apoyado por la comunidad científica, pues refuerzan la idea de que los pacientes pierden oportunidades en razón a que la ciencia progresa más rápido que el sistema de salud, lo cual impide desarrollar y dar mejor uso a las nuevas opciones de tratamiento. A su vez, permiten considerar que la protección de los datos del paciente y el uso secundario de los datos pueden lograrse al mismo tiempo¹⁵⁸.

El uso secundario de los datos es el que ocurre fuera de la prestación directa de atención médica¹⁵⁹, e implica una asociación entre individuos, considerados la fuente de los datos; los proveedores de atención médica, quienes recopilan los datos y tienen una relación de confianza con su paciente; los responsables de las políticas, que agrupan y usan los datos para desarrollar políticas en salud; e investigadores, quienes acceden y usan los datos para una variedad de propósitos, incluso para descubrir nuevas terapias¹⁶⁰.

2.3.1. Recomendaciones para la gobernanza de los datos personales de la salud. A continuación, se presentan las condiciones que la OCDE recomienda a los gobiernos establecer e implementar en un marco nacional de gobernanza aplicable al tratamiento de datos de la salud¹⁶¹.

2.3.1.1. Compromiso y participación de una amplia gama de partes interesadas. El tratamiento de datos personales de la salud debe contar con el compromiso y la participación, particularmente mediante consultas públicas, de una amplia gama de partes interesadas con el fin de garantizar que el procesamiento de los datos personales de salud sirva al interés público y sea coherente con los valores sociales y las expectativas razonables de las personas en cuanto a la protección y el uso de sus datos para la gestión del sistema de salud, investigación, estadísticas u otros fines relacionados con la salud que sirvan al interés público.

¹⁵⁶ KALKMAN, Shona, *et al.* Op. cit., p. 5.

¹⁵⁷ KOŠČÍK, Michal; MYŠKA, Matěj. Data protection and codes of conduct in collaborative research. [en línea]. En: International Review of Law, Computers & Technology, 2018, vol. 32, no. 1. [Citado en el 18 de mayo de 2019]. p. 145. Disponible en: <https://doi.org/10.1080/13600869.2018.1423888> [Traducido por la autora]

¹⁵⁸ EICHLER, Hans-Georg, *et al.* Op. cit., p. 919.

¹⁵⁹ SAFRAN, Charles, *et al.* Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. [en línea]. En: Journal of the American Medical Informatics Association, 2007, vol. 14, no. 1. [Citado en el 23 de mayo de 2019]. p. 2. Disponible en: <https://doi.org/10.1197/jamia.M2273> [Traducido por la autora]

¹⁶⁰ The Global Digital Health Partnership [GDHP]. Improving health insights. [en línea]. En: GDHP Whitepapers, 2019. [Citado en el 16 de junio de 2019]. p. 55. Disponible en: https://www.gdhp.org/media-hub/news_feed/gdhp-reports [Traducido por la autora]

¹⁶¹ OECD, Op. Cit, 2017c. p. 4-9

Para lograr que los sistemas de salud obtengan beneficios gracias a los datos, es necesario establecer confianza entre las partes interesadas¹⁶². Con su participación, es posible afrontar las dificultades que implica la transformación digital, mediante una asociación transparente y sinérgica orientada al cumplimiento de acuerdos y a la ejecución oportuna de las actividades requeridas¹⁶³.

Por ende, se necesita del análisis de quiénes son los interesados, cuáles son sus intereses y valores relevantes en cada contexto donde los datos de la salud son generados, usados y reutilizado, a fin de lograr el equilibrio entre derechos individuales, el potencial bien público que podría realizarse con la transformación digital, y los intereses de las empresas que esperan beneficiarse de actividades innovadoras¹⁶⁴.

2.3.1.2. Coordinación y cooperación de las partes interesadas. La OCDE recomienda la coordinación dentro del gobierno y la promoción de la cooperación entre organizaciones que procesan datos personales de salud en los sectores público o privado fomentando, por una parte, elementos y formatos de datos comunes, el aseguramiento de la calidad, y estándares de interoperabilidad de datos. Por otra, políticas y procedimientos comunes que minimicen las barreras para compartir datos, que sirvan al interés público, y protejan la privacidad y la seguridad de los datos.

Un modelo de atención en salud centrado en las personas, que permita a todos los agentes del sistema colaborar de manera informada y sincronizada, en orden a mejorar significativamente la seguridad de la atención en salud, necesita de la cooperación, apoyo e iniciativa de todos los agentes del sistema. Lo anterior, debido a que son ellos quienes guían el progreso dentro de sus organizaciones, establecen las prioridades, movilizan la experiencia, definen las estrategias y los requisitos de interoperabilidad para la compra de tecnología digital¹⁶⁵.

Por tanto, es necesario enfrentar en etapas tempranas de la digitalización del sector salud los desafíos relacionados con la coordinación y cooperación entre las partes interesadas. Lo anterior es posible regulando estándares para la interoperabilidad de los datos, a fin de garantizar la armonización de los requisitos técnicos. De tal manera, se puede asegurar que

¹⁶² OCDE. 2017b. Op. cit., p. 200.

¹⁶³ KIERKEGAARD, Patrick. Governance structures impact on eHealth. [en línea]. En: Health Policy and Technology, 2015, vol. 4, no. 1. [Citado en el 22 de junio de 2019]. p. 44. Disponible en: <https://doi.org/10.1016/j.hlpt.2014.10.016> [Traducido por la autora]

¹⁶⁴ SUNRISE WINTER, Jenifer; DAVIDSON, Elizabeth. Big data governance of personal health information and challenges to contextual integrity. [en línea]. En: The Information Society, 2019, vol. 35, no. 1. [Citado en el 3 de junio de 2019]. p. 47-48. Disponible en: <https://doi.org/10.1080/01972243.2018.1542648> [Traducido por la autora]

¹⁶⁵ PRONOVOST, Peter, *et. al.* Op. cit., p. 42.

la integración de la información en salud no resulte fragmentada, sino que sea significativa para el cumplimiento de los objetivos del sistema, a fin de obtener resultados duraderos¹⁶⁶.

2.3.1.3. Sistemas de datos de salud al servicio y protección del interés público. La OCDE recomienda revisar la capacidad de los sistemas de datos de salud del sector público usados para su tratamiento, para que sirvan y protejan el interés público. Esa revisión abarca criterios como la disponibilidad, calidad, aptitud para usar, accesibilidad, privacidad y seguridad de los datos. Particularmente, recomienda revisar que las transferencias de conjuntos de datos y la vinculación de los registros de conjuntos de datos se sujeten a salvaguardas apropiadas.

De acuerdo con la OCDE, los datos de la salud son considerados como fuente significativa de información para tomar decisiones encaminadas a mejorar la salud de la población, la efectividad, seguridad y la atención centrada en las personas¹⁶⁷.

Una condición importante en la digitalización de los sistemas de información de la salud se relaciona con su arquitectura, lo cual se refiere a los componentes que forman el sistema, sus propiedades y las relaciones entre tales componentes¹⁶⁸. Su importancia radica en dictar la cantidad y calidad de los datos, así como qué tan bien estos pueden ser compartidos, extraídos y analizados¹⁶⁹.

La recomendación de la OCDE refleja que, para lograr el potencial de los datos, es necesario invertir en la arquitectura de los sistemas de información, así como en capital humano y en experticia. Esa inversión permite afrontar problemas técnicos relacionados con la arquitectura de los sistemas de información, por ejemplo, el análisis de datos desestructurados, dada la inclusión de texto usando el vocabulario elegido por una persona, lo cual dificulta el análisis de los datos¹⁷⁰.

En cuanto a la seguridad de los datos, esta se puede mejorar empleando alternativas técnicas para su transferencia. A su vez, el acceso no autorizado o cualquier otro uso indebido es posible evitarlo mediante infraestructuras sólidas que dispongan de la verificación y autenticación de la identidad antes de otorgar el acceso a los datos.

¹⁶⁶ KIERKEGAARD, Patrick. Op. cit., p. 5.

¹⁶⁷ OCDE. Strengthening health information infrastructure matters. En: OCDE. Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges. Paris, 2013a [Citado en el 3 de mayo de 2019]. p. 18. Disponible en: <https://doi.org/10.1787/9789264193505-5-en>. [Traducido por la autora]

¹⁶⁸ MARIAM, Mikael Gebre, BYGSTAD, Bendik. Digitalization mechanisms of health management information systems in developing countries. [en línea]. En: Information and Organization, 2019, vol. 29, no. 1 [Citado en el 01 de junio de 2019]. p. 6. Disponible en: <https://doi.org/10.1016/j.infoandorg.2018.12.002> [Traducido por la autora]

¹⁶⁹ OCDE. 2017b. Op. cit., p. 199.

¹⁷⁰ OCDE. 2013a . Op. cit., p. 194.

2.3.1.4. Información para las personas. La OCDE recomienda brindar información clara a las personas para asegurar que, por una parte, conozcan de manera clara, precisa y en términos fácilmente comprensibles sobre el posible acceso a su información por parte de terceros; los objetivos del tratamiento; sus beneficios; y la base legal para ello. Por otra parte, que conozcan oportunamente cualquier violación de datos significativa u otro uso indebido de sus datos personales de salud. Cuando la notificación individual no sea practicable, esta podrá hacerse mediante comunicación pública efectiva.

La digitalización del sector salud promete mejorar eficiencias y expandir la capacidad de generar mayor conocimiento. Tienen un gran potencial para cambiar el rol de los pacientes, al promover su participación en el sistema de salud, así como para mejorar los resultados en salud¹⁷¹. Los usuarios del sistema pasan de ser receptores de información a tener un rol participativo, accediendo a información que previamente no era suministrada o era menos conocida, por ejemplo, mediante el acceso a su historia clínica electrónica.

Sin embargo, existen barreras que afectan la participación de los pacientes y al público en general en la digitalización del sector, por ejemplo, por la falta de motivación de las personas para comprender y mejorar su salud a través de datos electrónicos, por el desconocimiento de la tecnología o del valor que ofrece, lo que dificulta la participación especialmente de quienes tienen poca o ninguna experiencia en el uso de computadores o dispositivos móviles y carecen de las habilidades técnicas necesarias para ello¹⁷².

La transformación digital también puede generar daños únicos a la privacidad, por ejemplo, la analítica predictiva usando *big data*, que busca pronosticar los cambios en el estado de salud de las personas para así brindar atención médica y evaluar su posible consumo de recursos, puede llevar a predicciones que podrían usarse para excluir del acceso a la salud a las personas o poblaciones de alto costo¹⁷³.

De tal manera, cobra relevancia el proceso informativo de cara a los usuarios del sistema de salud, que les permita entender la transformación digital y decir si participan o no. En ese sentido, es necesario comprender cómo adaptar la práctica médica para preparar y educar a

¹⁷¹ GRÜNLOH, Christiane, *et al.* Why Do They Need to Check Me?" Patient Participation Through eHealth and the Doctor-Patient Relationship: Qualitative Study. [en línea]. En: Journal of medical internet research, 2018, vol. 20, no. 1. [Citado en el 19 de junio de 2019]. p. 2. Disponible en: <https://doi.org/10.2196/jmir.8444> [Traducido por la autora]

¹⁷² O'CONNOR, Siobhan, *et. al.* Understanding factors affecting patient and public engagement and recruitment to digital health interventions: a systematic review of qualitative studies. [en línea]. En: BMC Medical Informatics and Decision Making, 2016, vol 16, no. 120. [Citado en el 24 de julio de 2019.]. p. 6-8. Disponible en: <https://doi.org/10.1186/s12911-016-0359-3> [Traducido por la autora]

¹⁷³ SUNRISE WINTER, Jenifer; DAVIDSON, Elizabeth. Op. cit., p. 37

las personas, a fin de que puedan interpretar la información a la que acceden, mediante alternativas que apoyen a quienes no cuentan con conocimientos suficientes para ello¹⁷⁴.

2.3.1.5. Mecanismos para consentir el tratamiento de datos. La OCDE hace recomendaciones respecto de lo que deben proporcionar los mecanismos para consentir el tratamiento de datos, los cuales deben ser claros sobre si se requiere o no el consentimiento individual para procesar los datos personales de salud.

De requerirse el consentimiento, los mecanismos deben informar los criterios utilizados para tomar esta determinación, así como lo que constituye un consentimiento válido, cómo puede retirarse el consentimiento, las alternativas legales y excepciones a la exigencia de consentimiento, incluso en circunstancias donde obtenerlo sea imposible, impracticable o incompatible para lograr el propósito de interés público relacionado con la salud. El tratamiento de los datos debe sujetarse a salvaguardas compatibles con las recomendaciones de la OCDE.

Cuando el tratamiento de los datos personales de salud se base en el consentimiento, este se considera válido si se informa y se entrega libremente, y si se proporciona a los individuos mecanismos claros, visibles y fáciles de usar para proporcionar o retirar el consentimiento para el futuro uso de los datos.

Cuando el tratamiento de datos personales de salud no se base en el consentimiento, en la medida de lo posible, los mecanismos para consentir el tratamiento deben establecer que las personas puedan expresar sus preferencias con respecto al tratamiento de sus datos personales de salud, incluyendo capacidad de objetar en ciertas circunstancias, así como la capacidad de solicitar que sus datos se compartan para investigación u otro fin de interés público relacionado con la salud. Si las objeciones o solicitudes de tratamiento de datos no pueden ser atendidas, los mecanismos para consentir deben proporcionar a las personas los motivos de ello, incluida la base legal relevante.

La OCDE reconoce que los mecanismos para consentir el tratamiento de datos y las excepciones a su obtención varían de un país a otro. A su vez, un problema clave de los países OCDE frente al tratamiento de datos de la salud es la falta de claridad en cómo poner en práctica la legislación sobre protección de los datos, por ejemplo, en aspectos como el consentimiento informado¹⁷⁵.

Obtener el consentimiento del paciente es un requisito que presenta desafíos significativos para monitorear la salud y la atención médica, y para la investigación que involucre grandes

¹⁷⁴ WASS, Sofie; VIMARLUND, Vivian; ROS, Axel. Exploring patients' perceptions of accessing electronic health records: Innovation in healthcare. [en línea]. En: Health Informatics Journal, 2019, vol. 25, no. 1. [Citado en el 16 de junio de 2019]. p 211. Disponible en: <https://doi.org/10.1177/1460458217704258> [Traducido por la autora]

¹⁷⁵ OCDE. 2017b. Op. cit., p.199

poblaciones de pacientes y bases de datos. Ello porque las bases de datos del sistema de salud recopilan datos que representan a muchas personas y que sirven para otros fines, como administrar el sistema de salud o brindar atención clínica¹⁷⁶.

Por ello, cobra relevancia la comunicación clara y la transparencia al público acerca de por qué se recopilan los datos, a fin de mejorar la confianza de los pacientes en el sistema, lo que a su vez permite que las organizaciones recopilen datos de mejor calidad debido al mayor apoyo del paciente¹⁷⁷.

Aclarar la puesta en práctica de la legislación sobre protección de los datos resulta prioritario ante la transformación digital del sector salud. En las investigaciones que involucran humanos, se presupone la capacidad de indicar claramente al participante de la investigación sobre el uso y el propósito de tal actividad. Lo anterior es posible en estudios específicos, por ejemplo, cuando las personas son invitadas a participar en un ensayo clínico o encuesta¹⁷⁸.

Sin embargo, en las investigaciones que aplican tecnologías como *big data* se cambia el contexto del tratamiento de los datos, y las normas aplicadas en el contexto original del tratamiento pueden resultar irrelevantes en el segundo contexto. El consentimiento dado por el titular de los datos, si bien es el pilar para proteger la autonomía individual, se vuelve bastante vacío, y surge el riesgo de que pierda el control de sus datos cuando se usen para fines que no anticipó ni consintió, frustrando expectativas previas y ubicando a la persona simplemente como una fuente de datos, lo cual vulnera su dignidad¹⁷⁹.

2.3.1.6. Revisión y aprobación del uso de datos personales de salud para fines de investigación u otros de interés público relacionados con la salud. De acuerdo con la recomendación de la OCDE, los procedimientos para revisar y aprobar el uso de datos personales de salud para fines de investigación u otros de interés público relacionados con la salud deben: i) Implicar una evaluación basada en la evidencia de si el uso propuesto es de interés público; ii) Ser robustos, objetivos y justos; iii) Operar de manera oportuna y que promueva la consistencia de los resultados; iv) Operar de manera transparente mientras protege intereses legítimos; y v) Recibir el respaldo de una revisión multidisciplinaria independiente realizada por aquellos con la experiencia necesaria para evaluar los beneficios y riesgos del procesamiento para los individuos y la sociedad, y la mitigación de riesgos.

¹⁷⁶ OCDE 2015a. Op. cit., p. 78

¹⁷⁷ The Global Digital Health Partnership. Improving health insights. p. 54

¹⁷⁸ OCDE 2015a. Op. cit., p. 78

¹⁷⁹ BIRNHACK, Michael. A Process-based Approach to Informational Privacy and the Case of Big Medical Data. [en línea]. En: Theoretical Inquiries in Law, 2019, vol 20, no 1. [Citado en el 30 de mayo de 2019]. p. 268. Disponible en: <http://www7.tau.ac.il/ojs/index.php/til/article/view/1615> [Traducido por la autora]

El acceso a los datos de la salud puede ser bloqueado por restricciones de tipo legislativo, financiero y tecnológico, así como por la aversión al riesgo de compartir datos por parte de los responsables de los datos o los comités de ética¹⁸⁰. En orden a habilitar el acceso a los datos, esta recomendación de la OCDE refleja que la investigación en salud basa su legitimidad pública y aceptabilidad en su condición de iniciativa socialmente valiosa, realizada al servicio del bien público. Entonces, para garantizar la cooperación de las personas, es necesario informarles cómo se lleva a cabo y se regula la investigación, así como generar confianza en las instituciones y las personas que los reclutan¹⁸¹.

A su vez, se debe poner a disposición del público la descripción clara los flujos de datos, los acuerdos de intercambio de datos, los objetivos de la investigación, los resultados y su impacto clínico. Por ejemplo, los investigadores deben comunicar las razones por las cuales los sistemas de consentimiento están diseñados de determinada manera, así como las salvaguardas establecidas para controlar la privacidad del paciente, el proceso ético para acceder a los datos, la forma como se capacita a los equipos de investigación en materia de gobernanza, y las restricciones impuestas al acceso a los datos¹⁸².

Es clave informar e involucrar a cada una de las partes interesadas en habilitar el uso secundario de la información de salud, para determinar el interés por el uso de datos ahora y en el futuro, pues no involucrarlos puede tener consecuencias significativas cuando las personas sepan cómo se utilizan sus datos sin su conocimiento y permiso¹⁸³.

2.3.1.7. Mecanismos públicos de información para que el tratamiento sea transparente. Usar mecanismos públicos de información para que el tratamiento sea transparente, sin comprometer la privacidad de los datos, las medidas de seguridad o los intereses comerciales u otros legítimos de las organizaciones. La información pública debe incluir los siguientes elementos: i) Los propósitos, fines y base legal del procesamiento de los datos; ii) El procedimiento y los criterios utilizados para aprobar el procesamiento de datos de salud y un resumen de las decisiones de aprobación tomadas, incluida una lista de los receptores de datos aprobados; iii) Información sobre la implementación del marco de gobernanza de los datos de salud y su eficacia.

Esta recomendación se relaciona con la confianza que se necesita generar entre las partes interesadas, a fin de aprovechar al máximo los datos en la transformación digital del sector

¹⁸⁰ FORD, Elizabeth, *et. al.* Our data, our society, our health: A vision for inclusive and transparent health data science in the United Kingdom and beyond [en línea]. En: Learn Health Systems, 2019, vol. 3, no. 3. [Citado en el 24 de julio de 2019]. p. 3 Disponible en: <https://doi.org/10.1002/lrh2.10191> [Traducido por la autora]

¹⁸¹ CARTER, Pam; LAURIE, Graeme T; DIXON WOODS, Mary. The social licence for research: why care.data ran into trouble. [en línea]. En: Journal of Medical Ethics, 2015, vol. 41, no. 5. [Citado en el 11 de julio de 2019]. p. 406. Disponible en: <http://dx.doi.org/10.1136/medethics-2014-102374> [Traducido por la autora]

¹⁸² FORD, Elizabeth, *et. al.* Op. cit., p. 7.

¹⁸³ GDHP, 2019. Op. cit., p. 56.

salud. La OCDE considera que, para avanzar en la apertura de los datos para usos secundarios, se requiere implementar una estrategia de comunicación pública que sea abierta y transparente sobre los riesgos y beneficios generados con tales usos. Lo anterior permite que todas las partes interesadas conozcan qué datos serán recolectados, cómo serán usados, cómo y con quién podrán solicitar acceso a ellos, las condiciones de aprobación, requerimientos para la seguridad de los datos, y detalles de los procedimientos de investigación que sean aprobados¹⁸⁴.

2.3.1.8. Tecnología para la reutilización y el análisis de los datos. La OCDE recomienda maximizar el potencial y promover el desarrollo de la tecnología como un medio para permitir la reutilización y el análisis de los datos personales de salud, al tiempo que se protege la privacidad y la seguridad, facilitando a las personas el control sobre el uso de sus propios datos.

El uso secundario de los datos de la salud cobra importancia dada la creciente demanda para que los sistemas de salud usen datos del mundo real. Ahora bien, los sistemas actuales de ética y los procesos de aprobación regulatoria para la investigación se crearon en una época donde se dio poca importancia a las oportunidades de aprendizaje que podrían surgir del análisis secundario de los datos recopilados en la práctica diaria. Por tal motivo, los registros se mantienen escritos a mano, dispersos y desvinculados de otros consultorios médicos u hospitales, lo cual no brinda muchas oportunidades prácticas para el análisis secundario¹⁸⁵.

Entonces, para cumplir la demanda, los sistemas de salud necesitan que los datos obtenidos en la atención médica de rutina, principalmente contenidos en registros electrónicos generados en consultorios médicos de atención primaria, atención especializada y entornos hospitalarios, así como otros datos recopilados de forma rutinaria, transiten hacia información procesable. Lo anterior, acompañado de una estrategia de comunicación pública abierta y transparente sobre los riesgos y beneficios generados con tales usos.

2.3.1.9. Mecanismos de seguimiento y evaluación. La OCDE recomienda evaluar si los usos de datos personales de salud han cumplido con los propósitos de interés público relacionados con la salud y los beneficios esperados de tales usos; si se han producido consecuencias negativas como el incumplimiento de requisitos nacionales para la protección de la privacidad, de los datos personales de salud y la seguridad de datos, violaciones de datos, uso indebido de datos; y usar los resultados de dicha evaluación en un proceso de mejora continua, incluso a través de:

¹⁸⁴ OCDE. 2017b. Op. cit., p. 200-201

¹⁸⁵ EICHLER, Hans-Georg, *et. al.* Op. cit., p. 916

a) La revisión periódica de los desarrollos en la disponibilidad de datos de salud personales, las necesidades de investigación en salud y actividades relacionadas, y las necesidades de políticas públicas; y

b) La evaluación periódica y actualización de políticas y prácticas para gestionar la privacidad, la protección de los datos de salud personales y los riesgos de seguridad relacionados con el gobierno de dichos datos.

También recomienda alentar a quienes procesan datos personales de salud a revisar y evaluar periódicamente las capacidades, confiabilidad y vulnerabilidades de las tecnologías que utilizan.

2.3.1.10. Capacitación adecuada y el desarrollo de habilidades en medidas de privacidad y seguridad. Es recomendable establecer una capacitación adecuada y el desarrollo de habilidades en medidas de privacidad y seguridad para aquellos que procesan datos personales de salud, en línea con las normas y técnicas vigentes sobre tratamiento de datos.

El tratamiento de los datos de la salud se enfrenta a dificultades debido a la falta de oportunidades de capacitación, en razón a factores estructurales y logísticos que impiden ofrecer cursos efectivos. Esto ha resultado en una escasez de personas con habilidades y experiencia para innovar y maximizar los beneficios de los datos en salud, la cual resulta exacerbada a medida que la industria incrementa su demanda de personas capacitadas¹⁸⁶.

Estas dificultades necesitan ser abordadas adecuadamente para que el procesamiento y el uso secundario de los datos de la salud logren cambios sostenibles en la salud de la población. Al mismo tiempo, el tratamiento de los datos de la salud debe cumplir con el marco jurídico para aplicable a su protección, el cual debe reflejar los principios básicos de privacidad contenidos en las Directrices OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, así como cubrir todas las fuentes de datos, responsables y encargados del tratamiento.

En efecto, la seguridad de los datos y las prácticas de manejo son claves para cumplir los requisitos legales y las expectativas públicas. Por tanto, la capacitación adecuada y el desarrollo de habilidades en medidas de privacidad y seguridad permiten asegurar que los datos tratados estén a salvo, incluso durante cualquier transferencia y, en consecuencia, proteger la información de la salud.

2.3.1.11. Implementar controles y salvaguardas. Esta recomendación pretende que los marcos de gobernanza:

¹⁸⁶ FORD, Elizabeth, *et. al.* Op. cit., p. 4

- i) Proporcionen líneas claras y robustas de responsabilidad demostrada para el procesamiento de datos personales de salud, acompañados de mecanismos apropiados para la auditoría;
- ii) Establezcan requerimientos para que los datos personales de salud solo puedan ser procesados por, o ser responsabilidad de, organizaciones cuya totalidad de miembros cuente con capacitación adecuada en privacidad y seguridad de datos, de acuerdo con sus funciones y responsabilidades en el tratamiento de datos de la salud, y consistentes con los códigos de conducta profesionales que sean aplicables.
- iii) Promuevan en las organizaciones que procesan datos personales de salud a designar uno o varios empleados que coordinen y rindan cuentas del programa de seguridad de la información de la organización, incluido informar a la organización y sus empleados de sus obligaciones legales de proteger la privacidad y la seguridad de los datos.
- iv) Incluyan procesos formales de gestión de riesgos, actualizados periódicamente que evalúen y traten los riesgos, incluido el borrado no deseado de datos, la reidentificación¹⁸⁷, las violaciones u otros usos incorrectos, en particular al establecer nuevos programas o introducir prácticas novedosas.
- v) Incluyan medidas tecnológicas, físicas y organizacionales diseñadas para proteger la privacidad y la seguridad mientras se mantiene, en la medida de lo posible, la utilidad de los datos personales de salud para fines de interés público relacionados con la salud. Tales medidas deben incluir:
 - a. Mecanismos que limiten la identificación de las personas, incluso a través de la desidentificación¹⁸⁸ de sus datos personales de salud, y que tengan en cuenta el uso propuesto de los datos, al tiempo que también permitan la reidentificación cuando se apruebe. La reidentificación puede ser aprobada para realizar futuros análisis de datos para la gestión del sistema de salud, investigación, estadísticas u otros fines de interés público relacionados con la salud; o para informar a un individuo sobre una condición específica o resultado de la investigación, cuando sea apropiado.
 - b. Acuerdos cuando se compartan los datos personales de salud con terceros para su tratamiento, que ayuden a maximizar los beneficios y a administrar los riesgos, mientras se mantiene la utilidad de los datos. Tales acuerdos deben especificar las estipulaciones para la transferencia segura de datos e incluir medios apropiados para sancionar efectivamente el incumplimiento.

¹⁸⁷ Para los propósitos de la recomendación, el concepto *Reidentificación* significa el proceso por el cual la información es atribuida a datos desidentificados en orden a identificar al individuo que se relaciona con los datos desidentificados.

¹⁸⁸ Para los propósitos de la recomendación, el concepto *Desidentificación* fue definido como el proceso por el cual un conjunto de datos personales de la salud es alterado, y la información resultante no puede ser fácilmente asociada a individuos particulares. Los datos desidentificados no son datos anónimos.

c. Cuando sea practicable y apropiado, considerar alternativas a la transferencia de datos a terceros, tales como centros de acceso seguro de datos e instalaciones de acceso remoto a datos.

d. Verificación robusta de identidad y autenticación de individuos que acceden a datos personales de salud.

2.3.1.12. Demostrar cumplimiento de expectativas nacionales sobre gobernanza de los datos de salud. La OCDE recomienda requerir a las organizaciones que procesan datos personales de salud para demostrar que cumplen con las expectativas nacionales para la gobernanza de los datos de salud. Esto puede incluir el establecimiento de la certificación o acreditación de organizaciones que procesan datos personales de salud, en la medida en que estas certificaciones o acreditaciones ayuden a implementar estándares para el procesamiento de datos personales de salud o demuestren capacidad para cumplir con reconocidos estándares de gobernanza.

El auge de las tecnologías de internet durante el cambio de milenio, alentaron a las empresas a promover instrumentos de autorregulación como los contenidos en la recomendación de la OCDE, en orden a demostrar cumplimiento en materia de protección de datos¹⁸⁹. Ello obedeció a que instrumentos como la Directiva Europea de protección de datos (la Directiva 95/46 CE), no lograron abordar los desafíos que implicó el auge de Internet, mientras que los instrumentos de autorregulación, especialmente aquellos que regularon los flujos de datos transfronterizos entre Europa y los EE. UU., ofrecieron velocidad, flexibilidad y tal vez la oportunidad de posponer la intervención del legislador en esta actividad¹⁹⁰.

Desde entonces, en Europa existe una fuerte creencia en que instrumentos como la certificación garantizan la aplicación efectiva de la autorregulación, siendo así incorporada por el legislador europeo en la Sección 5 del Reglamento (UE) 2016/67979, como herramienta para demostrar la conformidad con el requisito general de responsabilidad establecido por la ley¹⁹¹.

2.3.2. Directrices OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Este instrumento contiene el primer conjunto de principios sobre privacidad acordados internacionalmente, enmarcados en un lenguaje conciso y neutral desde el punto

¹⁸⁹ LACHAUD, Eric. The General Data Protection Regulation and the rise of certification as a regulatory instrument. [en línea]. En: Computer law & security review, 2018, vol. 34, no. 2. [Citado en el 27 de julio de 2019]. p. 248. Disponible en: <https://doi.org/10.1016/j.clsr.2017.09.002> [Traducido por la autora]

¹⁹⁰ *Ibíd.* p. 249.

¹⁹¹ *Ibíd.* p. 250.

de vista tecnológico¹⁹², y sus destinatarios son los Estados miembros de la OCDE, a quienes se les recomienda implementarlas en sus leyes nacionales¹⁹³.

En el año 2013 fue adoptada la revisión y actualización de las directrices dados los cambios en el uso de datos personales y a los nuevos enfoques en la protección de la privacidad; revisión que resultó simultánea para tres de los marcos principales con dimensión internacional (OCDE, Unión Europea y Consejo de Europa)¹⁹⁴.

Varias prioridades llevaron a modernizar las Directrices OCDE, entre ellas, aumentar el enfoque en la evaluación práctica de los beneficios y riesgos asociados al uso de datos; evitar que la innovación fuese reprimida por leyes sobre privacidad de datos demasiado restrictivas o inflexibles; Hacer a los usuarios de los datos más responsables de los datos a los que acceden, almacenan y usan, y atribuirles responsabilidad cuando se produzcan daños a los individuos¹⁹⁵.

La revisión de las Directrices OCDE mantuvo los ocho principios orientadores contenidos en ella¹⁹⁶. También introdujo nuevos conceptos, como los programas de gestión de la privacidad, notificación de violaciones de seguridad, estrategias nacionales de privacidad, educación y sensibilización, y la interoperabilidad global. A su vez, ampliaron o actualizaron aspectos como la responsabilidad, los flujos transfronterizos de datos y la aplicación de la privacidad¹⁹⁷.

2.3.3. Aplicación del marco OCDE a Colombia

Colombia no es uno de los países adherentes a la Recomendación del Consejo de la OCDE sobre Gobernanza de los Datos de Salud. Entonces, podría considerarse que, en principio, dicho marco no le aplica.

Sin embargo, al iniciar su adhesión a la OCDE, el desempeño del sistema de salud colombiano fue evaluado en aspectos como su capacidad para brindar servicios seguros, apropiados a todos los grupos sociales y en forma oportuna, su sostenibilidad y

¹⁹² OCDE. The OECD privacy framework. [en línea]. 2013b. [Citado en el 18 de mayo de 2019]. p. 19. Disponible en: <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> [Traducido por la autora]

¹⁹³ KOŠČÍK, Michal; MYŠKA, Matěj. Op. cit., p. 144.

¹⁹⁴ OCDE. 2013b. Op. Cit., p. 21.

¹⁹⁵ CATE, Fred. H., CULLEN, Peter, MAYER-SCHÖNBERGER, Viktor. Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines. [en línea]. Books by Maurer Faculty, 2013. [Citado en el 21 de mayo de 2019]. p. 11. Disponible en: <https://www.repository.law.indiana.edu/facbooks/23/> [Traducido por la autora]

¹⁹⁶ Los principios contenidos en las Directrices OCDE son: Limitación de recogida; Calidad de los datos; Especificación del propósito; Limitación de uso; Salvaguardas de seguridad; Transparencia; Participación individual; Responsabilidad.

¹⁹⁷ OCDE. 2013b. Op. Cit., p. 22.

governabilidad, así como la responsabilidad y la transparencia de las partes interesadas involucradas en la toma de decisiones y la prestación de servicios de salud¹⁹⁸.

Con la evaluación se evidenció que al sistema de salud colombiano le falta información más detallada sobre la calidad del servicio y los resultados, siendo prioritario contar con información enfocada en los resultados de la atención primaria y los proveedores en general. Ello es prioridad porque los Prestadores de servicios de salud actualmente tienen muy pocos incentivos para mejorar su desempeño. Si bien existe el Sistema de Información Integral de la Protección Social (SISPRO), el público en general poco conoce la información allí disponible o cómo puede usarla para comparar proveedores y pagadores, lo que impide elegir de manera informada al asegurador y prestador de servicios. Igualmente, es necesario mejorar la calidad y comparabilidad de los datos para poder contrastarlos con los sistemas de salud de la OCDE¹⁹⁹.

La situación actual del sistema de salud colombiano, así como la situación general de los países OCDE, evidencian que los datos necesitan ser vistos como un recurso fundamental de los sistemas de salud, sociedades y de la comunidad global, no como un subproducto de los servicios de salud u otros como la administración o la facturación. Por ende, se requiere una transformación en la cultura y mentalidad por parte de todos los actores y partes interesadas: gobiernos, reguladores, proveedores, administradores y el público²⁰⁰.

CONCLUSIONES

- Los sistemas de atención en salud pertenecen a la industria de la información y el conocimiento, pues generan grandes cantidades de datos de diversos tipos. Sin embargo, su evolución en cuanto a estructura y gobernanza no se ha armonizado con su crecimiento en tamaño y complejidad. Lo anterior se refleja en la baja inversión en sistemas de información y en la poca información generada con los datos. En consecuencia, se pierde la oportunidad de monitorear e informar sobre la salud de la población, la calidad y seguridad de los servicios. Igualmente, se eleva el riesgo a que las personas experimenten una atención médica ineficiente, ineficaz e incluso perjudicial.
- La historia clínica electrónica integrada es una importante fuente de datos, razón por la cual la mayoría de los países miembro la están implementando dentro de un sistema nacional. Sin embargo, la preparación para gestionar los datos allí contenidos es baja en muchos países, por ejemplo, por problemas relacionados con la posibilidad de

¹⁹⁸ OCDE. Roadmap for the accession of Colombia to the OECD Convention. [en línea]. 2013c. [Citado en el 18 de mayo de 2019]. p. 18. Disponible en: [http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=c\(2013\)110/final&doclanguage=en](http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=c(2013)110/final&doclanguage=en) [Traducido por la autora]

¹⁹⁹ OCDE. Assessment and recommendations. En: OECD Reviews of Health Systems: Colombia, [en línea]. Paris, OECD Publishing, 2015b. [Citado en el 18 de mayo de 2019]. p. 21-22. Disponible en: <https://doi.org/10.1787/9789264248908-4-en> [Traducido por la autora]

²⁰⁰ OCDE. 2017b. Op. cit., p. 197

compartir los registros electrónicos entre los médicos de atención primaria y los especialistas.

- Para generar valor con el uso de los datos de la salud, estos deben ser combinados, armonizados, manejados y analizados. También se necesita invertir en infraestructura técnica, en capital humano, así como adoptar leyes que permitan afrontar los problemas clave a los que se enfrenta el tratamiento de datos de la salud en la era digital. Por ejemplo, los relacionados con los riesgos para la privacidad de las personas, así como para los individuos y sociedades cuando los activos de información no se desarrollan, no se usan o son muy difíciles de usar.
- La OCDE promueve ver los datos de la salud como un recurso fundamental de los sistemas de salud, sociedades y de la comunidad global, y no como un subproducto de los servicios de salud. Esta visión se orienta a que la protección de los datos del paciente y el uso secundario de los datos se logre al mismo tiempo. Ello genera que la gobernanza en materia de protección de datos, consentimiento, ética y acceso a los datos resulte ser mucho más exigente en el sector salud que en cualquier otro sector.
- Para países como Colombia, seguir la Recomendación OCDE sobre Gobernanza de los Datos de Salud, podría llevar a la generación de información enfocada en los resultados de la atención primaria y de los proveedores de servicios de salud en general, incentivando mejoras en su desempeño y la elección informada de aseguradores y prestadores de servicios de salud. Lo anterior es relevante dado que el país no cuenta con información detallada sobre la calidad y los resultados del servicio de salud, y es prioritario contar con canales claros y abiertos con las partes interesadas en el desarrollo y uso de los datos de la salud en razón a la creciente digitalización del tratamiento de los datos del sector.

3. LA PROTECCIÓN DEL DATO DE LA SALUD EN COLOMBIA FRENTE AL MARCO OCDE

INTRODUCCIÓN

Este capítulo está dedicado a contrastar algunos datos relacionados con la protección del dato de la salud en Colombia, frente a las condiciones que la OCDE recomienda a los gobiernos establecer e implementar en un marco nacional de gobernanza aplicable al tratamiento de datos de la salud. Para comenzar, se hace referencia al nivel de protección de dicho tratamiento en Colombia, y en seguida se concreta cada recomendación frente al contexto colombiano, a fin de identificar si la protección dada a los datos tratados por el sistema de salud colombiano resulta acorde con lo previsto por la Recomendación OCDE sobre gobernanza de los datos de salud.

3.1. NIVEL DE PROTECCIÓN DEL TRATAMIENTO DEL DATO DE LA SALUD EN COLOMBIA

En Colombia, la salud es protegida como un derecho fundamental que debe ser prestado de manera oportuna, eficaz y con calidad²⁰¹. La prestación del servicio de salud ocurre en el marco de un sistema altamente complejo, donde interactúan múltiples normas y agentes²⁰².

A pesar del reconocimiento normativo del derecho fundamental a la salud, Colombia ha presentado un incremento en cuanto a las acciones de tutela interpuestas para exigir el derecho a la salud a través de este mecanismo. Tal incremento ha sido interpretado como directamente proporcional a factores como el conocimiento que tienen los usuarios del sistema de salud respecto a sus derechos²⁰³.

En razón al volumen de casos abordados por la jurisprudencia, se reconoce la importancia de los datos del sistema de seguridad social en salud para el goce efectivo de múltiples derechos fundamentales²⁰⁴. Estos datos pueden estar contenidos en diferentes sistemas de información reglamentados por el Minsalud. Estos sistemas son poco conocidos por el público en general, no están integrados, tratan datos de baja calidad, y no cuentan con información detallada sobre la calidad de los servicios de salud y sus resultados²⁰⁵.

Los datos de la salud también están contenidos en la historia clínica, el documento más importante de toda la relación médico-paciente, que cuenta con información indispensable para brindar una atención integral²⁰⁶. Es el registro histórico de la atención dada a un individuo, e incide en la comunicación entre los diversos agentes del sistema de salud²⁰⁷. Allí se documenta el consentimiento informado, esto es, el proceso de comunicación entre el equipo de salud y el paciente, mediante el cual se defiende la dignidad y los derechos de los pacientes²⁰⁸.

A la historia clínica únicamente pueden acceder el usuario, el equipo de salud, las autoridades judiciales y de salud en los casos previstos en la ley, y las demás personas allí determinadas²⁰⁹, en razón a que es un documento privado sometido a reserva. También puede ser conocido por terceros, previa autorización otorgada por el paciente en forma expresa e inequívoca, debiendo en todo caso mantenerse la reserva legal.

²⁰¹ L.1751/2015, art. 2.

²⁰² ÁLVAREZ SALAZAR, Gabriel Jaime, GARCÍA GALLEGU, Marilyn, LONDOÑO USME, Maritza. Op. cit., p. 117

²⁰³ DEFENSORÍA DEL PUEBLO DE COLOMBIA. Op. cit., p. 89

²⁰⁴ UPEGUI MEJÍA, Juan Carlos. Op. Cit. p. 291.

²⁰⁵ OCDE. 2015b. Op. cit., p. 21-22.

²⁰⁶ CORREA MARTÍNEZ, César. Op. cit., p. 130.

²⁰⁷ OPS. 2016. Op. cit., p. 9.

²⁰⁸ ESCOBAR LÓPEZ, María Teresa; NOVOA TORRES, Edgar. Op. cit., p. 19.

²⁰⁹ R. 1995/1999, art. 1. literal a. MINSALUD

Los datos contenidos en la historia clínica y en los sistemas de información relativos a la salud son protegidos mediante normas relativas al tratamiento de datos de la salud, las historias clínicas y demás relacionadas con el tratamiento de datos personales. Dichas normas deben ser cumplidas por los sujetos involucrados en la recolección y uso de la información de la salud, de manera conjunta y armónica con la ley estatutaria sobre protección de datos²¹⁰.

A pesar de la existencia de los sistemas de información, los encargados de materializar el derecho a la salud tienen una ventaja informativa frente a los demás agentes del sistema, la cual incide en la creación de barreras administrativas asumidas por otros agentes, particularmente los usuarios²¹¹. Así pues, persisten ineficiencias en la prestación del servicio de salud, es difícil elegir de manera informada al asegurador y prestador de servicios²¹², así como reclamar medicamentos, obtener una cita médica, autorizar exámenes o intervenciones quirúrgicas²¹³.

Actualmente se promueve la implementación de la Historia Clínica Electrónica (HCE), dado el potencial que tiene para generar información relevante del sector salud²¹⁴. Su implementación podría mejorar la calidad y oportunidad de la atención, y proporcionar mejores datos sobre la efectividad y cobertura de las intervenciones en el sector salud²¹⁵.

Implementar la HCE en Colombia tiene potencial para mejorar la comunicación entre agentes y la eficiencia en la entrega de los servicios, así como promover la participación de los pacientes y mejorar los resultados en salud²¹⁶. Es también posible que genere cambios en la salud de la población en menor tiempo, ello mediante la operación conjunta entre fuentes de información y actores que integren los datos disponibles, los exploten y gestionen el conocimiento²¹⁷.

La explotación de datos de la salud mediante tecnologías como *big data* permiten una mejor identificación de patrones, comprender brotes epidemiológicos, predecir tendencias y

²¹⁰ REMOLINA ANGARITA, Nelson. Tratamiento de datos personales relativos a la salud: reflexiones en torno a la incidencia de la Ley 1581 de 2012 en el sector salud. Op. cit., p. 7-8.

²¹¹ ÁLVAREZ SALAZAR, Gabriel Jaime, GARCÍA GALLEGÓ, Marilyn, LONDOÑO USME, Maritza. Op. cit., p. 117-118.

²¹² OCDE. 2015b. Op. cit., p. 21-22.

²¹³ Exposición de motivos. Gaceta del Congreso. N° 98. 2019. Proyecto de ley número 233 de 2019 en Senado. Por medio del cual se racionalizan trámites en el sector salud, a través de la creación de la Historia Clínica Electrónica Única y se dictan otras disposiciones.

²¹⁴ OPS. 2016. Op. cit., p. 9.

²¹⁵ OMS. 2016. Op. cit., p. 6.

²¹⁶ OCDE. Understanding how the digital transformation affects people's well-being. En: How's Life in the Digital Age?: Opportunities and Risks of the Digital Transformation for People's Well-being. [en línea]. Paris: OECD Publishing, 2019. [Citado en el 11 de junio de 2019]. p. 22. Disponible en: <https://doi.org/10.1787/9789264311800-en> [Traducido por la autora]

²¹⁷ MINSALUD. Guía Metodológica para Registros, Observatorios, Sistemas de Seguimiento y Salas Situacionales Nacionales en Salud ROSS. Op. Cit., p. 119.

aplicar este conocimiento a los individuos para evaluar su trayectoria futura. Así mismo, el análisis de datos como los contenidos en la HCE, podría beneficiar a los pacientes, quienes recibirían un diagnóstico más rápido, preciso y un mejor tratamiento, así como a otras partes interesadas como empleadores, compañías de seguros, y el público en general²¹⁸.

Ahora bien, la mayor acumulación de datos en el sector salud crea nuevos riesgos relacionados con la privacidad y protección de datos sensibles, y surge un mayor interés por parte de terceros para acceder a tal información. En ese sentido, Colombia debe afrontar ciertos desafíos existentes a fin de obtener los beneficios esperados con la creciente digitalización del tratamiento de los datos generados en el sistema de salud.

Algunos desafíos presentes a nivel nacional consisten en mejorar la cultura de la información, afrontar el subregistro y la baja calidad de los datos, conocer y caracterizar mejor las fuentes de información, integrarlas y aumentar su trazabilidad, así como garantizar que la captación de datos, la formulación de políticas e intervenciones, y la evaluación del sistema de salud se haga según lineamientos de la OCDE²¹⁹.

Los desafíos a nivel internacional se relacionan con mejorar la disponibilidad de datos de la salud con calidad y que sean representativos para Colombia, conectar las fuentes de información con aquellas monitoreadas por organizaciones internacionales como la ONU, la OCDE, la OMS, así como incrementar la evidencia y literatura disponibles sobre Colombia en temas de interés de salud pública²²⁰.

La transformación digital también requiere de un marco jurídico que responda a los nuevos riesgos que representa. Por ejemplo, *big data* cambia el contexto del tratamiento de los datos, y las normas aplicadas en el contexto original del tratamiento pueden resultar irrelevantes en el segundo contexto. De ahí que el consentimiento dado por el titular de los datos se vuelva bastante vacío, y surja el riesgo de que pierda el control de sus datos cuando se usen para fines que no anticipó ni consintió, frustrando expectativas previas y ubicando a la persona simplemente como una fuente de datos, lo cual vulnera su dignidad²²¹.

La Superintendencia de Industria y Comercio, en calidad de autoridad nacional de protección de datos personales, considera que en Colombia no existe un vacío legislativo frente al tratamiento de información personal en sectores donde no existe una legislación específica o respecto del surgimiento de nuevas tecnologías o fenómenos tecnológicos²²². Sin embargo, la OCDE sugiere revisar los instrumentos legislativos que regulan el

²¹⁸ BIRNHACK, Michael. Op. Cit., p. 273.

²¹⁹ MINSALUD. Sistema de Evaluación del Desempeño del Sistema de Salud bajo Criterios OCDE COLOMBIA. Guía Metodológica. Bogotá, 2016, [Citado en el 3 de mayo de 2019]. p. 65-66. Disponible en: <https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VS/ED/GCFI/guia-ross-ocde.pdf>

²²⁰ *Ibíd.*, p. 65

²²¹ BIRNHACK, Michael. Op. Cit., p. 268.

²²² Cir. Ext. 04/2019, SIC, ANDJE.

tratamiento de los datos del sistema de salud, la privacidad y la seguridad, pues los existentes fueron desarrollados previo a la era digital²²³.

Por ejemplo la revisión podría orientarse a aclarar cómo poner en práctica la legislación sobre protección de los datos, por ejemplo, en aspectos como el consentimiento informado, el acceso a datos personales de la salud para investigación, y los efectos de hacer que los registros de salud estén disponibles para los pacientes²²⁴.

Aclarar estos aspectos es relevante para obtener los beneficios de digitalizar el tratamiento de los datos personales en el marco del sistema de salud colombiano, pues el análisis de factores como la necesidad de cada actor para acceder a los datos sensibles, por ejemplo, los contenidos en la historia clínica²²⁵, permite ajustar los instrumentos legislativos existentes para que respondan a los desafíos de la era digital.

Así pues, la transformación digital va más allá de la simple conversión de datos manuales a un formato digital. Implica transformar estructuras sociotécnicas, reconfigurar roles, relaciones, prácticas y estructuras organizacionales²²⁶. En ese sentido, resulta prioritario afrontar los desafíos y asuntos pendientes por aclarar, pues no abordar los riesgos de la transformación digital del sector salud dificulta los esfuerzos para que dicho sistema sea más eficiente mediante innovación²²⁷. También se puede perder la oportunidad de monitorear e informar sobre la salud de la población, la calidad y seguridad de los servicios, y la de investigar e innovar para mejorar los resultados de la atención médica. Incluso se puede perder la confianza pública en el gobierno, sus instituciones, y en el sistema de atención médica²²⁸.

3.2. TRATAMIENTO DE LOS DATOS DE LA SALUD EN COLOMBIA FRENTE A LA RECOMENDACIÓN OCDE

De acuerdo con la Organización para la Cooperación y el Desarrollo Económico (OCDE), la atención en salud pertenece a la industria de la información y el conocimiento, pues produce grandes cantidades de datos y de diversos tipos²²⁹. Sin embargo, los datos producidos no son aprovechados al máximo para generar información que ayude a lograr los objetivos de los sistemas de salud²³⁰.

Mediante la Recomendación sobre Gobernanza de los Datos de Salud, la OCDE promueve la transformación en la cultura y en la mentalidad de todos los actores y partes interesadas en el tratamiento de datos de la salud. En ese sentido, recomienda ajustes para lograr una

²²³ OCDE. 2017b. Op. cit., p. 199

²²⁴ GRÜNLOH, Christiane, *et al.* Op. cit., p. 2.

²²⁵ LÓPEZ, Joan. Op. Cit., p. 26

²²⁶ MARIAM, Mikael Gebre, BYGSTAD, Bendik. Op. cit., p. 1.

²²⁷ PRICE, William Nicholson. Op. Cit., p. 66.

²²⁸ *Ibíd.*, p. 88.

²²⁹ OCDE. 2017b. Op. cit. p. 187.

²³⁰ *Ibíd.*, p. 195.

fuerte gobernanza que soporte el tratamiento protector de la privacidad de los datos. Dichos ajustes se orientan al manejo más eficiente de la información de la salud, a fin de aprovechar al máximo los datos generados por esta industria, sin desconocer los beneficios y riesgos que ello representa²³¹.

La Recomendación de la OCDE es una de las iniciativas internacionales que existen en el ámbito de la salud digital, considerada como referente para la implementación efectiva de los servicios digitales de salud²³². Este instrumento de *Soft law* presenta doce recomendaciones aplicables al acceso y al procesamiento de datos personales de salud para fines de interés público relacionados con la salud. Así mismo, está dirigido a gobiernos e instituciones no gubernamentales y refleja que la gobernanza en materia de protección de datos, consentimiento, ética y acceso a los datos es mucho más exigente en el sector salud que en cualquier otro²³³.

Seguir ese tipo de recomendaciones no implica lograr la uniformidad entre las leyes adoptadas por los diversos Estados que adhirieron a ellas, lo cual puede resultar indeseable dadas sus diferencias culturales²³⁴. Ahora bien, en tanto referente para los servicios digitales de salud, el debate público de la Recomendación OCDE para la gobernanza de los datos personales de la salud podría orientar a la sociedad colombiana respecto a la transformación digital del sistema de salud, en orden a maximizar los beneficios y disminuir los riesgos que dicha iniciativa representa.

A continuación, se contrasta la recomendación OCDE frente al contexto colombiano, a fin de identificar si la protección dada a los datos tratados por el sistema de salud colombiano, resulta acorde con lo allí previsto.

3.2.1. Compromiso y participación de una amplia gama de partes interesadas. Para garantizar que el procesamiento de los datos personales de salud sirva al interés público y sea coherente con los valores sociales y las expectativas razonables de las personas, la OCDE recomienda que el tratamiento de datos personales de la salud debe contar con el compromiso y la participación de una amplia gama de partes interesadas.

En Colombia, el derecho fundamental a la salud comprende el derecho de las personas a participar en las decisiones adoptadas por los agentes del sistema de salud que los afectan o interesan. Este derecho se concreta en diversos escenarios de participación, como la formulación de la política de salud, los planes para su implementación, las instancias de

²³¹ OCDE. 2017b. Op. cit., p. 197

²³² The Global Digital Health Partnership. Improving health insights. p. 8

²³³ EICHLER, Hans-Georg, *et. al.* Hans-Georg, *et. al.* Op. cit., p. 917.

²³⁴ CATE, Fred. H., CULLEN, Peter, MAYER-SCHÖNBERGER, Viktor. Op. Cit. p. 14.

deliberación, veeduría y seguimiento del Sistema, las decisiones de inclusión o exclusión de servicios y tecnologías, entre otros²³⁵.

Así pues, la participación en salud se convierte en el motor de operatividad, dinamismo y verificación de la prestación de servicios de salud, propiciando a su vez la transparencia en la gestión del sistema. Sin embargo, la mayoría de los agentes del sector salud desconocen la estructura y funcionamiento de los mecanismos de participación ciudadana y comunitaria²³⁶. También existen serias dificultades para implementar las políticas, así como para reglamentar las leyes y hacer efectivo del derecho de las personas a participar en las decisiones adoptadas por los agentes del sistema, lo cual incide en que el verdadero acceso al derecho a la salud sea limitado²³⁷.

El Gobierno Colombiano ha identificado las problemáticas o necesidades en materia de participación en salud, que abarcan debilidades institucionales como la falta de direccionamiento estratégico y la visión medicalizada de la salud, la falta de cultura democrática, debilidades en capacidades ciudadanas, la fragmentación legal que incide en la instrumentalización de las normas, lo cual termina dando poder a quienes las apropian, convirtiéndose muchas veces en mecanismos de exclusión²³⁸.

Esa identificación de problemáticas llevó a la definición de la política de participación social en salud (PPSS), cuyos ejes estratégicos y líneas de acción se orientan al fortalecimiento institucional, el empoderamiento de la ciudadanía y las organizaciones sociales en salud, el impulso de la cultura de la salud, entre otros²³⁹. Así mismo, radicó en el Minsalud y en las entidades del sector a nivel nacional y territorial, en el nivel que sea de su competencia, realizar el seguimiento y evaluación de que permita identificar los alcances, logros y aprendizajes de la misma²⁴⁰.

3.2.2. Coordinación y cooperación de las partes interesadas. Integrar la transformación digital al sistema de salud de manera significativa y sin fragmentaciones, necesita de la

²³⁵ L. 1751/2015, art. 12

²³⁶ LÓPEZ AHUMADA, José Eduardo; RESTREPO PIMIENTA, Jorge Luis; GÓMEZ GÓMEZ, Marcela Lissette. Participación ciudadana en el Sistema de Seguridad Social en Salud: estudio de caso, percepciones de sus intervinientes en el departamento del Atlántico (Colombia). [en línea]. En: Reflexión Política, 2018, vol. 20, no. 39. [Citado en el 25 de junio de 2019]. p. 260. Disponible en: <https://doi.org/10.29375/01240781.3306>

²³⁷ MOLINA BULLA, Carlos Iván. Participación, políticas públicas, discapacidad mental/psicosocial y estigma: barreras y retos. [en línea]. En: Perspectivas em Políticas Públicas, 2018, vol. 11, no. 21. [Citado en el 30 de julio de 2019]. p. 189. Disponible en: <http://revista.uemg.br/index.php/revistappp/article/view/2891>

²³⁸ MINSALUD. Política de participación social en salud PPSS. Resolución 2063 de 2017. Bogotá, 2019. [Citado en el 4 de agosto de 2019]. p. 11-17. Disponible en: <https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/GT/politica-ppss-resolucion-2063-de-2017-cartilla.pdf>

²³⁹ *Ibíd.* p. 29-37.

²⁴⁰ *Ibíd.* p. 41. A la fecha en que se escribe este artículo, dichas entidades no han socializado los resultados de su seguimiento y evaluación.

coordinación dentro del gobierno y la cooperación entre organizaciones que procesan datos personales de salud. Lo anterior implica adoptar elementos y formatos de datos comunes, así como estándares de interoperabilidad, en orden a garantizar la calidad de los datos.

Esta recomendación refleja que, para aprovechar los datos de la salud, es necesario que estos sean comparables y puedan usarse para fines de monitoreo e investigación. De tal manera, la estructura de los datos, los estándares de contenido, y la capacidad para compartir los datos se convierten en factores clave para la transformación digital en el sector salud²⁴¹.

Una gran cantidad de agentes reportan información al sistema de salud colombiano, lo cual genera complejidad en el flujo de información. A su vez, el sistema cuenta con varios niveles para agregar datos según la entidad a la que se reporta, produciendo así duplicidades, bajas coberturas y poca calidad en los datos sin mecanismos de retroalimentación al respecto. Adicionalmente, la información se encuentra almacenada en bodegas de datos aisladas, con problemas de interoperabilidad técnica, semántica y de infraestructura, debido a que en Colombia los sistemas de información se han desarrollado de manera fragmentada²⁴².

Además, la interoperabilidad de la información de la salud en Colombia no se ha desarrollado de manera uniforme. Por una parte, Bogotá cuenta con avances en la estandarización, a nivel de historia clínica electrónica, de los tipos de información intercambiada por las entidades de la red de atención pública²⁴³. Por otra parte, el Gobierno está desarrollando el proyecto para lograr la interoperabilidad de la historia clínica a nivel nacional, pero aún falta desarrollar los lineamientos y las condiciones tecnológicas requeridas para ello²⁴⁴.

3.2.3. Sistemas de datos de salud al servicio y protección del interés público. La OCDE recomienda revisar la capacidad de los sistemas de datos de salud del sector público usados para su tratamiento, a fin de que sirvan y protejan el interés público. Esta revisión se refiere a factores como la disponibilidad, calidad, aptitud para usar, accesibilidad, privacidad y seguridad de los datos. Respecto de las transferencias de conjuntos de datos y la vinculación de los registros de conjuntos de datos, la OCDE recomienda que estas actividades se sujeten a salvaguardas apropiadas.

Los sistemas de datos de salud existentes en Colombia contienen información que es proporcionada por diversos agentes del sector, y que podrían considerarse pertinentes y

²⁴¹ OCDE. 2017b. Op. cit., p. 208-209.

²⁴² ESLAVA RINCÓN, Julia, *et al.* Op. cit., p. 9-11

²⁴³ LÓPEZ SEVILLANO, Alexandra María, SALCEDO PARRA, Octavio José, REYES DAZA, Brayan. Op. cit., p. 12.

²⁴⁴ Concepto jurídico del Ministerio de Salud y Protección Social al Proyecto de Ley número 233 de 2019. Senado. Gaceta del Congreso 403. 2019. p. 11

suficientes para el seguimiento del acceso, uso y calidad de los servicios de salud. Sin embargo, es difícil hacer seguimiento del sistema de salud con la información allí almacenada, pues esta desarticulada, segmentada y proporciona datos desactualizados, de baja calidad o ineficientes²⁴⁵ lo que, sumado al desconocimiento de los registros estandarizados en el sistema, genera poco uso de la información a pesar de su existencia²⁴⁶.

3.2.4. Información para las personas. La digitalización del sector salud tiene un gran potencial para cambiar el rol de los pacientes, al promover su participación en el sistema de salud, así como para mejorar los resultados en salud²⁴⁷. A su vez, puede generar daños únicos a la privacidad, razón por la cual cobra relevancia el proceso informativo de cara a las personas usuarias del sistema de salud.

Por ello, la OCDE recomienda brindar información a las personas para asegurar que, por una parte, conozcan de manera clara, precisa y en términos fácilmente comprensibles sobre el posible acceso a su información por parte de terceros; los objetivos del tratamiento; sus beneficios; y la base legal para ello. Por otra parte, que conozcan oportunamente cualquier violación de datos significativa u otro uso indebido de sus datos personales de salud. Cuando la notificación individual no sea practicable, esta podrá hacerse mediante comunicación pública efectiva.

La recomendación resulta importante puesto que, mediante el acceso a la información de la salud y en particular a la contenida en la historia clínica electrónica, los usuarios del sistema adquieren un rol más participativo²⁴⁸. De ahí que sea necesario prepararlos y educarlos para que puedan interpretar la información a la que acceden, así como afrontar las deficiencias que actualmente existen respecto al consentimiento informado requerido para la atención en salud, dadas sus complejidades y a que generalmente se limita a un documento que en muchos casos sirve para cumplir con un requisito legal, pero que no implica una apropiación del proceso comunicativo de información por parte del paciente²⁴⁹.

Respecto de la recomendación de informar a las personas sobre cualquier violación de datos significativa u otro uso indebido de sus datos personales de salud, la Ley 1581 de 2012 dispone que los responsables y encargados del tratamiento de datos deben notificar a la autoridad de protección de datos, en caso de cualquier violación de la seguridad y existencia de riesgos en la gestión de datos personales, pero no obliga informar a los interesados, aunque esto es alentado por la autoridad de protección de datos²⁵⁰.

²⁴⁵ SUÁREZ ROZO, Luisa Fernanda, *et al.* Op. cit., p. 48

²⁴⁶ ESLAVA RINCÓN, Julia, *et al.* Op. cit., p. 9-11

²⁴⁷ GRÜNLOH, Christiane, *et al.* Op. cit., p. 2.

²⁴⁸ WASS, Sofie; VIMARLUND, Vivian; ROS, Axel. Op. cit., p 211.

²⁴⁹ ESCOBAR LÓPEZ, María Teresa; NOVOA TORRES, Edgar. Op. cit., p. 17-19.

²⁵⁰ LEHUEDÉ, Héctor J. Op. cit., p. 43.

3.2.5. Mecanismos para consentir el tratamiento de datos. La OCDE plantea recomendaciones respecto de lo que deben proporcionar los mecanismos para consentir el tratamiento de datos, los cuales deben ser claros sobre si se requiere o no el consentimiento individual para procesar los datos personales de salud. Igualmente, precisa sus recomendaciones dependiendo de si se requiere o no el consentimiento.

Un problema clave de los países OCDE frente al tratamiento de datos de la salud, es la falta de claridad en cómo poner en práctica la legislación sobre protección de los datos, por ejemplo, en aspectos como el consentimiento informado²⁵¹. Los mecanismos para consentir el tratamiento de datos y las excepciones a su obtención varían de un país a otro. Estos mecanismos a su vez contienen exigencias en materia de protección de datos, consentimiento, ética y acceso a los datos en el sector salud, mucho más exigentes que en cualquier otro sector²⁵².

El marco jurídico colombiano regula las condiciones en que debe administrarse, conservarse, custodiarse y mantener la confidencialidad de los datos de la salud, particularmente los contenidos en la historia clínica. Este marco dispone como necesario solicitar al titular su consentimiento expreso para suministrar los datos personales a terceros, a fin de proteger la confidencialidad y la privacidad de los sujetos.

Igualmente, la Ley 1581 de 2012 y el Decreto reglamentario 1377 del 2013 permiten usar la información sin el consentimiento del titular cuando: ello obedezca a una finalidad histórica, estadística o científica; cuando se trate de urgencias médicas o sanitaria; cuando los datos se hayan recolectado antes de la expedición de la norma; se trate de datos de naturaleza pública; cuando dicha autorización imponga una carga desproporcionada derivada de la obligación de solicitar a cada titular la autorización para usar sus datos personales, o cuando el responsable no cuente con los datos de contacto de los titulares²⁵³.

En Colombia se ha reconocido que el marco jurídico aplicable al tratamiento de los datos personales debe ajustarse, pues no responde a los nuevos riesgos que surgen en contextos como el de la explotación de datos²⁵⁴.

No obstante, por parte de la autoridad nacional de protección de datos aún no se ha visibilizado la necesidad de actualizar el marco jurídico o de evaluar la efectividad de las normas sobre debido tratamiento de los datos personales. Tal evaluación resulta necesaria, por ejemplo frente al consentimiento informado requerido para la protección de datos de la

²⁵¹ OCDE. 2017b. Op. cit., p.199

²⁵² EICHLER, Hans-Georg, *et. al.* Op. cit., p. 917

²⁵³ LOPERA, Mónica María. Revisión comentada de la legislación colombiana en ética de la investigación en salud. [en línea]. En: Biomédica, 2017, vol. 37, no. 4. [Citado en el 8 de julio de 2019]. p. 584-585. Disponible en: <https://doi.org/10.7705/biomedica.v37i4.3333>

²⁵⁴ Documento CONPES 3920. p. 58.

salud, especialmente ante los nuevos riesgos que trae la digitalización del tratamiento de datos del sector salud con la implementación de la historia clínica electrónica.

A lo anterior se suma que los formatos usados para documentar el consentimiento informado de personas sometidas a procedimientos frecuentes en la atención en salud, no cumplen con parámetros legales o principios bioéticos, pues no existe un verdadero acompañamiento para informar de manera clara y oportuna para crear verdaderos canales de comunicación con las personas. Lo anterior se refleja en la falta de información sobre riesgos o ventajas y desventajas de los tratamientos, así como de las consecuencias en caso de negativa o tardanza en dar el consentimiento, o el uso de lenguaje técnico y de un elevado número de frases, palabras y contenido²⁵⁵.

3.2.6. Revisión y aprobación del uso de datos personales de salud para fines de investigación u otros de interés público relacionados con la salud. La OCDE identifica cinco componentes para la revisión y aprobación del uso de datos personales de salud, para fines de investigación u otros de interés público relacionados con la salud. Estos componentes implican una evaluación basada en la evidencia de si el uso propuesto es de interés público. A su vez, deben ser robustos, objetivos y justos, deben operar de manera oportuna, transparente, y deben recibir el respaldo de una revisión multidisciplinaria independiente, realizada por aquellos con la experiencia necesaria para evaluar los beneficios y riesgos del procesamiento para los individuos y la sociedad, y la mitigación de riesgos.

La investigación en salud actualmente se rige en Colombia por normas que no contemplan aspectos éticos de la investigación surgidos en las últimas décadas y, para algunos temas tratados, lo reglamentado es insuficiente. Por ejemplo, la investigación donde se apliquen técnicas de revisión documental retrospectiva, revisión de historias clínicas, entrevistas, cuestionarios y otros, corresponde a la categoría de investigaciones sin riesgo. Dicha categoría asume que, con la revisión documental, la aplicación de cuestionarios y la realización de entrevistas, nunca se pondría en riesgo el anonimato y la autodeterminación de los participantes²⁵⁶.

3.2.7. Mecanismos públicos de información para que el tratamiento sea transparente. Para provechar al máximo los datos en la transformación digital del sector salud, es necesario generar confianza entre las partes interesadas. De ahí que se requiera implementar una estrategia de comunicación pública abierta y transparente sobre los riesgos y beneficios generados con tales usos, para así avanzar en la apertura de los datos, especialmente para usos secundarios²⁵⁷.

²⁵⁵ ESCOBAR LÓPEZ, María Teresa; NOVOA TORRES, Edgar. Op. cit., p. 27-32.

²⁵⁶ MATEUS, Julio Cesar, *et al.* Op. cit., p. 16.

²⁵⁷ OCDE. 2017b. Op. cit., p. 200-201

Por esta razón, la OCDE recomienda usar mecanismos públicos para que el tratamiento sea transparente, los cuales deben informar sobre los propósitos, fines y base legal del procesamiento de los datos; el procedimiento y los criterios utilizados para aprobarlo y un resumen de las decisiones de aprobación tomadas, incluida una lista de los receptores de datos aprobados; la implementación del marco de gobernanza de los datos de salud y su eficacia. El uso de estos mecanismos no debe comprometer la privacidad de los datos, las medidas de seguridad o los intereses comerciales u otros legítimos de las organizaciones.

La experiencia colombiana refleja que se necesitan acciones concretas en orden a lograr que el tratamiento de datos de la salud sea transparente. En el año 2018, el Gobierno Colombiano propuso la creación del Sistema de Información Clínica y Laboral. Este sistema buscaba solucionar los problemas de comunicación entre prestadores de servicios de salud, generados cada vez que los pacientes visitan a diferentes prestadores. También se orientaba a facilitar el acceso a la telemedicina en zonas apartadas del país, así como a garantizar un gobierno abierto para la innovación y la construcción de política pública mediante datos, a fin de generar mayor eficiencia en el sistema de salud mediante su digitalización²⁵⁸.

Dicha propuesta incluyó a la historia clínica electrónica en los Servicios Ciudadanos Digitales, con el objetivo de optimizar y facilitar el adecuado acceso de los usuarios a la administración pública a través de medios electrónico. Los servicios ciudadanos digitales hacen parte de una iniciativa orientada a permitir que los colombianos archiven y consulten documentos clave para sus interacciones con el Estado, por ejemplo, documentos como la historia clínica²⁵⁹.

Aunque la propuesta no es fuente jurídica vigente, su publicación evidenció que en su preparación faltó analizar quiénes y para qué deben acceder a los datos personales sensibles de una persona, contenidos en su historia clínica electrónica. El análisis de dichos asuntos resulta necesario puesto que al colocar la historia clínica en el ecosistema de los servicios ciudadanos digitales, parece ubicarla dentro de una estructura de datos cada vez más privatizada del Estado en general, y que existiría por fuera del Sistema de Salud²⁶⁰.

3.2.8. Tecnología para la reutilización y el análisis de los datos. En razón a las grandes cantidades de datos que son generadas por los sistemas de salud, la OCDE promueve que estos datos sean transformados en información que ayude a lograr los objetivos de los sistemas²⁶¹.

No obstante, los datos obtenidos en la atención médica aún se mantienen escritos a mano, dispersos y desvinculados de otros consultorios médicos u hospitales, lo cual no brinda

²⁵⁸ LÓPEZ, Joan. Op. cit. p. 15

²⁵⁹ OCDE. 2017a. Op. cit., p. 28.

²⁶⁰ LÓPEZ, Joan. Op. cit. p. 28-29

²⁶¹ OCDE. 2017b. Op. cit., p. 205

muchas oportunidades prácticas para el análisis secundario, pues se trata de información que no es procesable²⁶². Además, aún existen problemas para compartir entre médicos de atención primaria y especialistas los registros contenidos en la Historia Clínica Electrónica (HCE), a pesar de que su nivel de implementación es alto en muchos países de la OCDE y su acceso es considerado como el factor que habilita en gran medida el uso secundario de los datos de la salud²⁶³.

Por consiguiente, la OCDE recomienda maximizar el potencial y promover el desarrollo de la tecnología, como un medio para permitir la reutilización y el análisis de los datos personales de salud, al tiempo que se protege la privacidad y la seguridad, facilitando a las personas el control sobre el uso de sus propios datos.

A pesar de que Colombia es uno de los países miembro de la OMS que aún no cuenta con HCE²⁶⁴, en el país se reconoce que los datos son un insumo para la actividad investigativa, académica y productiva. Por esta razón, el Minsalud adoptará un mecanismo electrónico que desarrolle la interoperabilidad de la historia clínica, a fin de que las personas relacionadas con la atención en salud compartan los datos definidos por el Gobierno nacional²⁶⁵.

Ahora bien, en el proceso de reglamentar los sistemas de información interoperables, particularmente la HCE, ni el Gobierno así como tampoco la academia o la sociedad civil, han socializado datos que permitan identificar el espectro de riesgos que implica tratar los datos de la salud en ese tipo de sistemas, quedando los operadores de los servicios ciudadanos digitales a cargo de definir las medidas apropiadas, efectivas y verificables que les permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales.

3.2.9. Mecanismos de seguimiento y evaluación. Los datos de la salud son considerados como datos de carácter reservado, en razón a que su divulgación puede dar lugar a conductas discriminatorias, las cuales potencialmente pueden causar perjuicios a su titular²⁶⁶. Estos perjuicios pueden concretarse en ámbitos financieros, por ejemplo, mediante la discriminación en el aseguramiento de la salud o el empleo; psicosociales, como vergüenza, estigma y pérdida de reputación, derivando a su vez en aislamiento y estrés; pérdida de la confianza pública en el gobierno y sus instituciones, incluso en el sistema de salud²⁶⁷.

²⁶² EICHLER, Hans-Georg, *et. al.* Op. cit., p. 916

²⁶³ OCDE. 2017b. Op. cit., p. 208.

²⁶⁴ OMS. 2016. Op. cit., p. 2.

²⁶⁵ L. 1955/2019, art. 246

²⁶⁶ TRAVIESO Juan Antonio. Op. cit., p. 920.

²⁶⁷ OCDE. 2013a. Op. cit., p. 88.

En ese sentido, la OCDE recomienda evaluar si el uso de los datos personales de salud ha cumplido con los propósitos de interés público y los beneficios esperados; si se han producido consecuencias negativas como el incumplimiento de requisitos nacionales para la protección de la privacidad, de los datos personales de salud y la seguridad de datos, violaciones de datos, uso indebido de datos; y usar los resultados de dicha evaluación en un proceso de mejora continua. También alienta a quienes procesan datos personales de salud a revisar y evaluar periódicamente las capacidades, confiabilidad y vulnerabilidades de las tecnologías que utilizan.

La transformación digital del tratamiento de datos del sector salud, por ejemplo, mediante la analítica predictiva usando *big data*, puede pronosticar cambios en el estado de salud de las personas en orden a brindarles atención médica y evaluar su posible consumo de recursos, y también puede generar daños únicos a la privacidad que lleven a predicciones que podrían usarse para excluir del acceso a la salud a las personas o poblaciones de alto costo²⁶⁸.

En Colombia, los riesgos generados en razón a la acumulación desproporcionada de información personal por perfiles y categorías han sido reconocidos jurisprudencialmente, pero no se encuentran reflejados en la ley ni en la regulación de protección de datos, así como tampoco en el documento Conpes sobre la Política de Explotación de Datos, pues en este instrumento no se incluyeron medidas específicas para prevenir las consecuencias discriminatorias del perfilamiento²⁶⁹.

En cuanto al marco jurídico aplicable a las investigaciones en salud, si bien la ley estatutaria sobre protección de datos personales dispone que los datos relativos a la salud corresponden a la categoría de datos sensibles que afectan la intimidad del Titular o un uso indebido puede generar su discriminación²⁷⁰, la investigación en salud donde basada en la revisión de historias clínicas, entre otros documentos, son consideradas como investigaciones sin riesgo, a pesar de que existe la posibilidad de que se ponga en riesgo el anonimato y la autodeterminación de los participantes en ese tipo de investigación²⁷¹.

3.2.10. Capacitación adecuada y el desarrollo de habilidades en medidas de privacidad y seguridad. La generación de valor mediante el tratamiento de datos de la salud necesita de inversiones en cuanto a capital humano²⁷², puesto que la falta de personas capacitadas genera escasez de habilidades y experiencia para innovar y maximizar los beneficios de los

²⁶⁸ SUNRISE WINTER, Jenifer; DAVIDSON, Elizabeth. Op. cit., p. 37

²⁶⁹ GONZÁLEZ GUERRERO, Laura Daniela. Control de nuestros datos personales en la era del *big data*: el caso del rastreo web de terceros. [en línea]. En: Estudios Socio-Jurídicos, 2018, vol. 21, no. 1. [Citado en el 4 de julio de 2019]. p. 223-224. Disponible en: <http://dx.doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941>.

²⁷⁰ L.1581/2012, art. 5.

²⁷¹ MATEUS, Julio Cesar, *et al.* Op. cit., p. 16.

²⁷² OCDE, 2013a, Op. cit., p. 194

datos en salud²⁷³. De ahí que la OCDE recomiende establecer una capacitación adecuada y el desarrollo de habilidades en medidas de privacidad y seguridad para aquellos que procesan datos personales de salud, en línea con las normas y técnicas vigentes sobre tratamiento de datos.

En el marco del gobierno digital en Colombia, las entidades públicas del orden nacional perciben diferencias entre ellas, en cuanto a los avances en la implementación de los sistemas de información, así como en la capacitación recibida para gestionar la información. Estas diferencias también son percibidas como limitaciones para implementar la plataforma de interoperabilidad, que es el mecanismo para estandarizar los flujos de datos entre entidades²⁷⁴.

Por ello, Colombia necesita asegurar una visión estratégica coherente para todo el gobierno y la sociedad, mediante la creación de capacidades humanas e institucionales que se orienten a generar disponibilidad de las competencias y los recursos requeridos para ejecutar proyectos como el de la historia clínica electrónica, en orden a que se logre su adopción efectiva²⁷⁵.

3.2.11. Implementar controles y salvaguardas. Encontrar el equilibrio entre las reglas para la protección de los datos, particularmente entre privacidad y transparencia, es una tarea continua que lleva varias décadas en desarrollo, donde la privacidad generalmente ha tenido una ventaja sobre la transparencia. En ocasiones, los derechos de las personas pueden haber estado expuestos a daños injustificados en aras de la transparencia. En muchas otras ocasiones, las consideraciones de privacidad han impedido el acceso público a la información que habría contribuido a un mejor funcionamiento de la democracia, o una sociedad menos corrupta²⁷⁶.

Ahora bien, los diversos controles y salvaguardas recomendadas por la OCDE para la gobernanza de los datos de la salud permiten equilibrar privacidad y transparencia, al tiempo que reflejan que la atención en salud se rige por expectativas de responsabilidad y normas de pertenencia y comportamiento, cuyo cumplimiento necesita de ciertas inversiones para aumentar la conciencia pública sobre las diferentes formas en que se

²⁷³ FORD, Elizabeth, *et. al.* Op. cit., p. 4

²⁷⁴ Documento CONPES 3920. p. 47-51

²⁷⁵ OCDE. Implementación coherente de políticas de gobierno digital en contextos diferentes en Colombia. En: Revisión del Gobierno Digital en Colombia: Hacia un Sector Público Impulsado por el Ciudadano, Paris, 2018. [Citado en el 3 de noviembre de 2019]. p. 109 - 134. Disponible en: <https://dx.doi.org/10.1787/9789264292147-7-es>

²⁷⁶ LEHUEDÉ, Héctor J. Corporate governance and data protection in Latin America and the Caribbean. [en línea]. Santiago, Production Development series, No. 223 (LC/TS.2019/38), Comisión Económica para América Latina y el Caribe (CEPAL), 2019. [Citado en el 4 de julio de 2019]. p. 31-32. Disponible en: <http://hdl.handle.net/11362/44629> [Traducido por la autora]

concreta la digitalización del sector salud, junto con la comprensión de cómo estas funcionan, qué beneficios pueden aportar y los posibles riesgos²⁷⁷.

Implementar un marco regulatorio apropiado para las nuevas realidades de la era digital no es fácil, y los Estados modernos carecen de los medios y las capacidades para realizar esta función. Por ello, la nueva normalidad implica presenciar coaliciones más diversas de actores que brindan soluciones “contingentes”, donde los reguladores abandonan una fijación sobre la finalidad y la seguridad jurídica y adoptan la contingencia, la flexibilidad y la apertura a lo nuevo²⁷⁸.

En ese sentido, la OCDE recomienda implementar controles y salvaguardas, mientras se mantiene en la medida de lo posible, la utilidad de los datos personales de salud para fines de interés público relacionados con la salud. Dentro de los controles y salvaguardas se encuentra el establecimiento de líneas claras y sólidas de responsabilidad demostrada, así como de mecanismos apropiados para la auditoría. En cuanto al procesamiento de los datos, esta actividad debe ser ejecutada por las organizaciones cuya totalidad de miembros cuenten con capacitación adecuada en privacidad y seguridad de datos. Igualmente, en el procesamiento se deben cumplir los códigos de conducta profesionales que sean aplicables, siendo uno o varios empleados quienes coordinen y rindan cuentas del programa de seguridad de la información de la organización.

También recomienda incluir procesos formales de gestión de riesgos, actualizados periódicamente que evalúen y traten riesgos como el borrado no deseado de datos, la reidentificación de los datos o violaciones u otros usos incorrectos. Esta recomendación resulta de particular importancia cuando se establezcan nuevos programas o se introduzcan prácticas novedosas, en razón a factores como la facilidad con que los datos pueden ser reidentificación en el mundo digital²⁷⁹.

En cuanto a las medidas tecnológicas, físicas y organizacionales diseñadas para proteger la privacidad y la seguridad de los datos, la OCDE recomienda incluir mecanismos robustos para verificar la identidad y autenticación de los individuos que acceden a datos personales de salud, así como mecanismos que limiten la identificación de las personas, incluso a través de la desidentificación de sus datos personales, teniendo en cuenta el uso propuesto. La reidentificación de los datos recomienda la OCDE que pueda ser aprobada para realizar futuros análisis para la gestión del sistema de salud, investigación, estadísticas u otros fines

²⁷⁷ O’CONNOR, Siobhan, *et. al.* Op. cit., p. 10

²⁷⁸ FENWICK, Mark, VERMEULEN, Erik P. The Lawyer of the Future as “Transaction Engineer”: Digital Technologies and the Disruption of the Legal Profession. [en línea]. En: CORRALES, M., FENWICK, M., HAAPIO H. (Eds). Legal Tech, Smart Contracts and Blockchain. Perspectives in Law, Business and Innovation. Singapur, Springer, 2019. [Citado en el 21 de mayo de 2019]. p. 266. Disponible en: https://doi.org/10.1007/978-981-13-6086-2_10 [Traducido por la autora]

²⁷⁹ BIRNHACK, Michael. Op. cit., p. 284.

de interés público relacionados con la salud; o para informar a un individuo sobre una condición específica o resultado de la investigación, cuando sea apropiado.

Sobre la posibilidad de compartir los datos personales de salud con terceros para su tratamiento, la OCDE recomienda contar con acuerdos que ayuden a maximizar los beneficios y a administrar los riesgos, mientras se mantiene la utilidad de los datos. Estos acuerdos deben especificar las estipulaciones para la transferencia segura de datos e incluir medios apropiados para sancionar efectivamente el incumplimiento. Además, recomienda cuando sea práctico y apropiado, considerar alternativas a la transferencia de datos a terceros, tales como centros de acceso seguro de datos e instalaciones de acceso remoto a los datos.

En Colombia, los responsables y encargados de tratar datos personales pueden ejecutar dicha actividad de acuerdo con una finalidad específica, durante el tiempo necesario y razonable para cumplirla. Cumplida la finalidad, deberán suprimir el dato personal, salvo que para el cumplimiento de una disposición legal o contractual se requiera su conservación. Así mismo, deben implementar las medidas técnicas, humanas y administrativas que resulten idóneas para garantizar la seguridad de las bases de datos, especialmente para evitar que la información sea adulterada, se pierda, sea usada, consultada o accedida sin autorización o de manera fraudulenta²⁸⁰.

Así mismo, la Superintendencia de Industria y Comercio (SIC) en su guía para la implementación del principio de responsabilidad demostrada sugiere que, para demostrar la adopción de medidas internas efectivas y apropiadas para garantizar la protección de los datos, dentro de la organización debe existir una estructura administrativa directamente proporcional a la estructura y el tamaño del responsable del tratamiento. Adicionalmente, deben existir mecanismos internos en orden a implementar la política para el tratamiento, deben brindar capacitación a los empleados y responder a las solicitudes de los interesados, así como las juntas directivas y los altos directivos deben participar activamente en el desarrollo, implementación y verificación del cumplimiento en materia de protección de datos²⁸¹.

3.2.12. Demostrar cumplimiento de expectativas nacionales sobre gobernanza de los datos de salud. Los desafíos creados en la época de auge de las tecnologías de internet llevaron a que las empresas promovieran instrumentos de autorregulación, para abordar tales desafíos y a la vez poder demostrar su cumplimiento en materia de protección de datos²⁸². Estos instrumentos fueron incorporados por el legislador europeo para que mediante ellos se

²⁸⁰ Concepto 18865701/2018. SIC

²⁸¹ LEHUEDÉ, Héctor J. Op. cit., p. 43

²⁸² LACHAUD, Eric. Op. cit., p. 249.

podiera demostrar la conformidad con el requisito general de responsabilidad establecido para la protección de datos²⁸³.

De modo similar, la OCDE recomienda que las organizaciones que procesan datos personales de salud demuestren su cumplimiento con las expectativas nacionales para la gobernanza de los datos de salud. Tal demostración puede ocurrir mediante la certificación o acreditación de las organizaciones que procesan datos personales de salud, herramientas que pueden ayudar a implementar estándares para el procesamiento de los datos o demostrar capacidad para cumplir con reconocidos estándares de gobernanza.

En Colombia, la creación de confianza en las partes interesadas en el tratamiento de datos personales puede resultar de la obtención de certificaciones de buenas prácticas. Ahora bien, no hay normatividad aplicable a estas certificaciones, razón por la cual su expedición se rige por los estándares de las organizaciones certificadoras de carácter internacional, las cuales se relacionan con metodologías de manejo de la información así como también con temas de seguridad y aseguramiento de la información, como es el caso de la certificación ISO/IEC 27000 del 2018 sobre seguridad e información y sistemas de gestión, o la norma técnica ISO/IEC 27001 sobre el manejo de los sistemas y la implementación del *Data Protection Compliance*²⁸⁴.

3.3. AJUSTES PARA MEJORAR LA GOBERNANZA DE LOS DATOS DE LA SALUD EN COLOMBIA

Los datos de la salud atienden intereses públicos que abarcan los ámbitos de la salud, la justicia, la industria, la ciencia, la innovación y las finanzas²⁸⁵. Son datos producidos en un sector que pertenece a la industria de la información y el conocimiento, pero que está rezagado en el aprovechamiento de los datos, debido a que las sociedades no están acostumbradas a generar información valiosa para lograr los objetivos de los sistemas de salud²⁸⁶.

Colombia ha emprendido acciones para avanzar hacia el aprovechamiento de los datos de la salud, y se espera que con los Servicios Ciudadanos Digitales el país cuente con las capacidades y eficiencias requeridas, a fin de optimizar y facilitar el adecuado acceso de los usuarios del sistema a la historia clínica electrónica (HCE). En efecto, le corresponde al

²⁸³ *Ibíd.*, p. 250.

²⁸⁴ MONCADA ZAPATA, Juan Carlos. Siete aspectos legales en torno a la relación compliance y tratamiento de datos personales. [diapositivas]. Colombia: VII Congreso Internacional de Protección de Datos Personales, 2019. p. 9.

²⁸⁵ OCDE. 2017c. Op. cit., p. 12.

²⁸⁶ *Ibíd.*, p. 195.

MinTIC, definir y expedir los estándares, modelos, lineamientos y normas técnicas para la incorporación de las TIC aplicables a los servicios ciudadanos digitales, incluida la HCE²⁸⁷.

Por su parte, la Corporación Agencia Nacional Digital (AND) es la entidad encargada de articular los servicios ciudadanos digitales²⁸⁸, lo cual implica adelantar las interacciones con los distintos actores involucrados para lograr una prestación coordinada y adecuada de tales servicios²⁸⁹. A la AND también le corresponde definir las condiciones del sistema, educar a la ciudadanía, otorga concesiones a las empresas operadoras del sistema, así como vigilar y controlar al Operador, que es la persona jurídica prestadora de los servicios ciudadanos digitales²⁹⁰.

La experiencia de los países miembro de la OCDE refleja que progresar en la implementación de la HCE, se relaciona con factores como la existencia de un marco jurídico que permita extraer de las HCE los datos para fines estadísticos y de investigación, sujeto a las garantías adecuadas, así como el análisis de los datos extraídos de la HCE en función a los objetivos nacionales clave de monitoreo e investigación²⁹¹.

Ahora bien, al contrastar la Recomendación OCDE del año 2017 para la gobernanza de los datos personales de la salud frente al contexto colombiano es posible identificar que, en Colombia, se requieren algunos ajustes para que la protección dada a los datos tratados por el sistema de salud colombiano resulte acorde con lo previsto en la Recomendación.

Realizar los ajustes que a continuación se describen puede favorecer la implementación efectiva de los servicios digitales de salud²⁹², así como también permiten maximizar los beneficios y minimizar los riesgos derivados del tratamiento del dato de la salud, mediante el desarrollo de una fuerte gobernanza enmarcada normativamente, que permita tratar los datos de la salud para fines de investigación, estadísticos y para mejorar la calidad de la atención de salud²⁹³.

Para garantizar que el procesamiento de los datos personales de la salud en Colombia sirva al interés público y sea coherente con los valores sociales y las expectativas razonables de las personas, es fundamental implementar estrategias para contar con el compromiso y la participación de una amplia gama de partes interesadas y de tal manera, hacer efectivo el acceso a la participación ciudadana en el sector salud, mediante la construcción de

²⁸⁷ L. 1753/2015, art. 45.

²⁸⁸ D. 2257/2017, art. 1.

²⁸⁹ D. 1413/2017, que adiciona al D. 1078/2015 el art. 2.2.17.1.3. núm. 2.

²⁹⁰ D. 1413/2017, que adiciona al D. 1078/2015 el art. 2.2.17.1.3. núm. 16.

²⁹¹ OCDE. 2017b. Op. cit., p. 205

²⁹² The Global Digital Health Partnership. Improving health insights. p. 8

²⁹³ *Ibíd.*, p. 1.

confianza entre las partes²⁹⁴, a fin de equilibrar los derechos individuales, el potencial bien público que se busca con el tratamiento de los datos y los intereses involucrados²⁹⁵.

Este ajuste obedece a que el desarrollo de los sistemas de información de la salud que soportan su tratamiento debe realizarse mediante consulta abierta y transparente con todas las partes interesadas, en orden a que estos sistemas reflejen valores sociales relacionados con los derechos a la privacidad y a la salud, siendo igualmente accesibles para usos secundarios sujetos a medidas de seguridad.

El procesamiento y uso secundario de los datos de la salud está permitido si su objetivo se relaciona con asuntos de salud pública, investigación y estadísticos. En ese sentido, el marco jurídico sobre protección de datos debe incluir medidas de seguridad que reflejen los principios contenidos en las Directrices OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, que cubra todas las fuentes de datos, responsables y encargados del tratamiento, y que sea actualizado para reflejar los valores sociales conforme evoluciona y cambia el panorama de la salud.

También se necesita adoptar elementos y formatos de datos comunes, así como estándares para la interoperabilidad de los datos, en orden a garantizar su calidad y permitir que sean comparables y se puedan extraer fácilmente para usos de monitoreo e investigación. Con ello, es posible asegurar que la integración de la información en salud sea significativa para el cumplimiento de los objetivos del sistema, a fin de obtener resultados duraderos²⁹⁶.

Colombia necesita invertir en la arquitectura de los sistemas de información de la salud, para lograr que los datos generados puedan ser compartidos, extraídos y analizados²⁹⁷. Igualmente, se requiere afrontar problemas técnicos como el análisis de datos desestructurados, así como estudiar alternativas técnicas para que su transferencia sea segura, por ejemplo, mediante infraestructuras sólidas para la verificación y autenticación de la identidad previa al otorgamiento del acceso a los datos²⁹⁸.

Para brindar información clara a los usuarios del sistema de salud colombiano, se requiere superar las barreras que dificultan la participación especialmente de quienes carecen de las habilidades técnicas necesarias²⁹⁹. Así mismo, es pertinente adaptar la práctica médica para preparar y educar a las personas, a fin de que puedan interpretar la información a la que acceden, mediante alternativas que apoyen a quienes no cuentan con conocimientos suficientes para interpretar dicha información³⁰⁰.

²⁹⁴ OCDE. 2017b. Op. cit., p. 200.

²⁹⁵ SUNRISE WINTER, Jenifer; DAVIDSON, Elizabeth. Op. cit., p. 47-48.

²⁹⁶ KIERKEGAARD, Patrick. Op. cit., p. 5.

²⁹⁷ OCDE. 2017b. Op. cit., p. 199.

²⁹⁸ OCDE. 2013a. Op. cit., p. 194.

²⁹⁹ O'CONNOR, Siobhan, *et. al.* Op. cit., p. 6-8.

³⁰⁰ WASS, Sofie; VIMARLUND, Vivian; ROS, Axel. Op. cit., p. 211.

También se necesita mejorar el acto de comunicación en el marco de la atención en salud, en orden a obtener el consentimiento informado que cumpla con los parámetros legales y principios bioéticos. Lo anterior permite mejorar la confianza de los pacientes en el sistema, al tiempo que se protege su autonomía individual y su dignidad, así como también permite que las organizaciones recopilen datos de mejor calidad debido al mayor apoyo del paciente³⁰¹.

En razón a que la investigación en salud basa su legitimidad pública y aceptabilidad en su condición de iniciativa socialmente valiosa, realizada al servicio del bien público, es necesario informarles a las personas cómo se lleva a cabo y se regula la investigación, para así garantizar su cooperación y generar confianza en las instituciones y las personas que los reclutan³⁰². Por consiguiente, es necesario revisar y actualizar las normas colombianas que regulan la investigación en salud, para que cubran todo el espectro de investigación, particularmente lo planteado en materia de investigación que implique el tratamiento de datos contenidos en la historia clínica³⁰³.

El sistema de salud colombiano necesita contar con mecanismos públicos que informen sobre los riesgos y beneficios generados por el uso de los datos, en orden a que el tratamiento sea transparente y no comprometa la privacidad, las medidas de seguridad o los intereses comerciales u otros legítimos de las organizaciones. Esos mecanismos permitirán generar confianza entre las partes interesadas, así como aprovechar al máximo los datos en la transformación digital del sector salud.

Para que la historia clínica electrónica efectivamente logre ser implementada, debe involucrarse a todas las partes interesadas en orden a que sea el bienestar de las personas el elemento determinante, más no los intereses políticos que prioricen aspectos como la reducción de costos en la implementación de la tecnología³⁰⁴. Lo anterior es relevante dado que la historia clínica electrónica en el servicio de carpeta ciudadana podrá beneficiar a todas las partes interesadas mediante la capacitación adecuada y el desarrollo de habilidades en medidas de privacidad y seguridad de quienes traten los datos personales de salud.

Cobra relevancia evaluar el uso de los datos personales de salud en cuanto al cumplimiento de los propósitos de interés público y los beneficios esperados, así como detectar la producción de consecuencias negativas y usar los resultados de dicha evaluación en un proceso de mejora continua en la medida en que dicha evaluación permita que el análisis predictivo sea transparente, así como también permita evitar que la atención médica sea brindada con base en datos errados o discriminatorios.

³⁰¹ The Global Digital Health Partnership. Improving health insights. p. 54

³⁰² CARTER, Pam; LAURIE, Graeme T; DIXON WOODS, Mary. Op. cit., p. 406.

³⁰³ MATEUS, Julio Cesar, *et al.* Op. cit., p. 27.

³⁰⁴ KIERKEGAARD, Patrick. Op. cit., p. 6

Igualmente se requiere implementar controles y salvaguardas, mientras se mantiene en la medida de lo posible, la utilidad de los datos personales de salud para fines de interés público relacionados con la salud mediante herramientas que ayuden a implementar estándares para el procesamiento de datos personales de salud, y demostrar capacidad para cumplir con reconocidos estándares de gobernanza.

CONCLUSIONES

- La Recomendación del Consejo de la OCDE sobre Gobernanza de los Datos de Salud es considerada como referente para la implementación efectiva de los servicios digitales de salud. Al contrastar su contenido con algunos datos del contexto colombiano, se identificaron situaciones que ameritan ajustes para que la protección dada a los datos tratados por el sistema de salud colombiano logre maximizar los beneficios y disminuir los riesgos de la digitalización del tratamiento de los datos personales.
- Colombia no es uno de los países adherentes a la recomendación ODCE, lo cual podría explicar por qué el gobierno no hace referencia a dicha recomendación en los documentos relacionados con la reglamentación de la Historia Clínica Electrónica en el marco de los Servicios Ciudadanos Digitales. Esa falta de documentación no permite identificar si Colombia está considerando implementar el instrumento en la digitalización del tratamiento de los datos personales del sector salud.
- Uno de los ajustes identificados consiste en contar con el compromiso y la participación de una amplia gama de partes interesadas y de tal manera, hacer efectivo el acceso a la participación ciudadana en el sector salud. A la fecha en que se escribe este artículo, las entidades a cargo de realizar el seguimiento y evaluación para identificar los alcances, logros y aprendizajes de la política de participación social en salud (PPSS) no han socializado los resultados de su seguimiento y evaluación. Tampoco se cuenta con documentación sobre la evaluación del marco jurídico colombiano aplicable al tratamiento de datos, para identificar si su alcance y efectividad responden a los nuevos riesgos relacionados con la privacidad y protección de los datos sensibles.
- Falta focalizar la transformación digital hacia la generación de beneficios para la sociedad, especialmente para los usuarios del sistema de salud, quienes son los que asumen las barreras administrativas generadas por las asimetrías de información en el sector salud. Ello es relevante puesto que la imposibilidad de superar las ineficiencias en la prestación del servicio de salud con la información disponible, podría ser una de las razones del aumento de las acciones de tutela interpuestas para exigir la efectividad del derecho a la salud. Igualmente, la focalización permite identificar estrategias para la construcción de confianza pública, necesaria para que la transformación digital genere valor público y beneficie a la sociedad.

BIBLIOGRAFÍA

LIBROS Y ARTÍCULOS

ÁLVAREZ SALAZAR, Gabriel Jaime, GARCÍA GALLEGO, Marilyn, LONDOÑO USME, Maritza. Crisis de la salud en Colombia: limitantes del acceso al derecho fundamental a la salud de los adultos mayores. [En línea]. En: Revista CES Derecho, 2016, vol. 7, no. 2, [Citado en el 3 de mayo de 2019]. 116-125 p. Disponible en: <http://dx.doi.org/10.21615/cesder.7.2.8>

BERNAL ACEVEDO, Oscar, FORERO CAMACHO, Juan Camilo. Sistemas de información en el sector salud en Colombia. En: Revista Gerencia y políticas de salud, 2011, vol. 10, no. 21. [Citado en el 3 de mayo de 2019]. 85-100 p. Disponible en: <https://revistas.javeriana.edu.co/index.php/gerepolsal/article/view/2590>

BIRNHACK, Michael. A Process-based Approach to Informational Privacy and the Case of Big Medical Data. [en línea]. En: Theoretical Inquiries in Law, 2019, vol. 20, no 1. [Citado en el 30 de mayo de 2019]. 257-290 p. Disponible en: <http://www7.tau.ac.il/ojs/index.php/til/article/view/1615>

BOTERO CABRERA, Carolina. Las historias de los Servicios Ciudadanos Digitales. En: El espectador. Bogotá, 27 de Julio de 2019. Disponible en: <https://www.elespectador.com/opinion/las-historias-de-los-servicios-ciudadanos-digitales-columna-873130>

CARTER, Pam; LAURIE, Graeme T; DIXON WOODS, Mary. The social licence for research: why care.data ran into trouble. [en línea]. En: Journal of Medical Ethics, 2015, vol. 41, no. 5. [Citado en el 11 de julio de 2019]. 404 - 409 p. Disponible en: <http://dx.doi.org/10.1136/medethics-2014-102374>

CASTAÑEDA, Juan Diego. ¿Otra vez la misma historia? Cuando las TIC se interponen entre la ciudadanía y el Estado. Disponible en: <https://karisma.org.co/otrashistorias/documentation/otra-vez/>

CATE, Fred. H., CULLEN, Peter, MAYER-SCHÖNBERGER, Viktor. Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines. [en línea]. Books by Maurer Faculty, 2013. [Citado en el 21 de mayo de 2019]. 23 p. Disponible en: <https://www.repository.law.indiana.edu/facbooks/23/>

CORREA MARTÍNEZ. César. La historia clínica. Aspectos jurídicos y dilemas en el derecho español y colombiano. [en línea]. En: VIEI, 2015, vol. 10, no. 2. 125-144 p. Disponible en: <https://doi.org/10.15332/s1909-0528.2015.0002.03>

CRAWFORD, Kate, SCHULTZ Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. [en línea]. En: Boston College Law Review, 2014, vol.

55, no. 93 [Citado en el 8 de mayo de 2019]. 93-128 p. Disponible en:
<http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>

DEFENSORÍA DEL PUEBLO DE COLOMBIA. La tutela y los derechos a la salud y a la seguridad social. 13 ed., Bogotá, 2019. 188 p.

EICHLER, Hans-Georg, et. al. Data Rich, Information Poor: Can We Use Electronic Health Records to Create a Learning Healthcare System for Pharmaceuticals? [en línea]. En: *Clinical Pharmacology & Therapeutics*, 2018, vol. 105, no. 4, [Citado en el 23 de mayo de 2019]. 912-922 p. Disponible en: <https://doi.org/10.1002/cpt.1226>

ESCOBAR LÓPEZ, María Teresa; NOVOA TORRES, Edgar. Análisis de formatos de consentimiento informado en Colombia. [en línea]. En: *Revista Latinoamericana de Bioética*, 2016, vol. 30, no. 1. [Citado el 22 de julio de 2019]. 14-37 p. Disponible en: <https://doi.org/10.18359/rlbi.1439>

ESLAVA RINCÓN, Julia, et al. 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. [en línea]. En: *Revista Gerencia y políticas de salud*, 2018, vol. 17, no 35, [Citado en el 3 de mayo de 2019]. 16 p. Disponible en: <https://doi.org/10.11144/Javeriana.rgps17-35.acrs>

FENWICK, Mark, VERMEULEN, Erik P. The Lawyer of the Future as “Transaction Engineer”: Digital Technologies and the Disruption of the Legal Profession. [en línea]. En: CORRALES, M., FENWICK, M., HAAPIO H. (Eds). *Legal Tech, Smart Contracts and Blockchain. Perspectives in Law, Business and Innovation*. Singapur, Springer, 2019. [Citado en el 21 de mayo de 2019]. 253-272 p. Disponible en: https://doi.org/10.1007/978-981-13-6086-2_10

FORD, Elizabeth, et. al. Our data, our society, our health: A vision for inclusive and transparent health data science in the United Kingdom and beyond [en línea]. En: *Learn Health Systems*, 2019, vol. 3, no. 3. [Citado en el 24 de julio de 2019]. 1-12 p. Disponible en: <https://doi.org/10.1002/lrh2.10191>

GALLOR LINARES, Luisa Manuela; HERNÁNDEZ MONROY, Daniela Alexandra; NIETO VANEGAS, Jineth Alejandra. Explicación y análisis del Sistema de Seguridad Social en Salud en Colombia. [en línea]. En: *Revista Digital Isocuanta*, 2017 vol. 2, no. 11. [Citado en el 01 de junio de 2019]. 11-20 p. Disponible en: <https://revistas.usantotomas.edu.co/index.php/isocuanta/article/view/4330>

GONZÁLEZ GUERRERO, Laura Daniela. Control de nuestros datos personales en la era del *big data*: el caso del rastreo web de terceros. [en línea]. En: *Estudios Socio-Jurídicos*, 2018, vol. 21, no. 1. [Citado en el 4 de julio de 2019]. 209-244 p. Disponible en: <http://dx.doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941>.

GRÜNLOH, Christiane, et al. Why Do They Need to Check Me?" Patient Participation Through eHealth and the Doctor-Patient Relationship: Qualitative Study. [en línea]. En: Journal of medical internet research, 2018, vol. 20, no. 1. [Citado en el 19 de junio de 2019]. 14 p. Disponible en: <https://doi.org/10.2196/jmir.8444>

KALKMAN, Shona, et al. Responsible data sharing in international health research: a systematic review of principles and norms. [en línea]. En: BMC Med Ethics, 2019, vol. 20, no. 21. [Citado en el 20 de mayo de 2019]. 13 p. Disponible en: <https://doi.org/10.1186/s12910-019-0359-9>

KIERKEGAARD, Patrick. Governance structures impact on eHealth. [en línea]. En: Health Policy and Technology, 2015, vol. 4, no. 1. [Citado en el 22 de junio de 2019]. 39-46 p. Disponible en: <https://doi.org/10.1016/j.hlpt.2014.10.016>

KOŠČÍK, Michal; MYŠKA, Matěj. Data protection and codes of conduct in collaborative research. [en línea]. En: International Review of Law, Computers & Technology, 2018, vol. 32, no. 1. [Citado en el 18 de mayo de 2019]. 141-154 p. Disponible en: <https://doi.org/10.1080/13600869.2018.1423888>

LACHAUD, Eric. The General Data Protection Regulation and the rise of certification as a regulatory instrument. [en línea]. En: Computer law & security review, 2018, vol. 34, no. 2. [Citado en el 27 de julio de 2019]. 244-256 p. Disponible en: <https://doi.org/10.1016/j.clsr.2017.09.002>

LEHUEDÉ, Héctor J. Corporate governance and data protection in Latin America and the Caribbean. [en línea]. Santiago, Production Development series, No. 223 (LC/TS.2019/38), Comisión Económica para América Latina y el Caribe (CEPAL), 2019. [Citado en el 4 de julio de 2019]. 66 p. Disponible en: <http://hdl.handle.net/11362/44629>

LOPERA, Mónica María. Revisión comentada de la legislación colombiana en ética de la investigación en salud. [en línea]. En: Biomédica, 2017, vol. 37, no. 4. [Citado en el 8 de julio de 2019]. 577-589 p. Disponible en: <https://doi.org/10.7705/biomedica.v37i4.3333>

LÓPEZ AHUMADA, José Eduardo; RESTREPO PIMIENTA, Jorge Luis; GÓMEZ GÓMEZ, Marcela Lisette. Participación ciudadana en el Sistema de Seguridad Social en Salud: estudio de caso, percepciones de sus intervinientes en el departamento del Atlántico (Colombia). [en línea]. En: Reflexión Política, 2018, vol. 20, no. 39. [Citado en el 25 de junio de 2019]. 254-262 p. Disponible en: <https://doi.org/10.29375/01240781.3306>

LÓPEZ, Joan. Servicios ciudadanos digitales e historias clínicas electrónicas. [en línea]. Bogotá, 2019. [Citado en el 17 de mayo de 2019]. 35 p. Disponible en: <https://karisma.org.co/otrashistorias/documentation/scd-hce/>

LÓPEZ SEVILLANO, Alexandra María, SALCEDO PARRA, Octavio José, REYES DAZA, Brayan. Análisis del estado actual de la salud pública bajo el marco de la interoperabilidad. [en línea]. En: Revista científica Puente, 2015. vol. 9, no. 2. [Citado en el

3 de mayo de 2019]. 13 p. Disponible en:
<https://revistas.upb.edu.co/index.php/puente/article/view/7104>

MARIAM, Mikael Gebre, BYGSTAD, Bendik. Digitalization mechanisms of health management information systems in developing countries. [en línea]. En: Information and Organization, 2019, vol. 29, no. 1 [Citado en el 01 de junio de 2019]. 1-22 p. Disponible en: <https://doi.org/10.1016/j.infoandorg.2018.12.002>

MATEUS, Julio Cesar, *et al.* Resolución 8430 de 1993: ¿Responde a las necesidades actuales de la ética en investigación en salud con seres humanos en Colombia? [en línea]. En: Biomédica, 2019, vol. 39, no. 3. [Citado en el 8 de julio de 2019]. p. 16. Disponible en: <https://www.revistabiomedica.org/index.php/biomedica/article/view/4333>

Ministerio de Salud y Protección Social [MINSALUD]. Interoperabilidad para una propuesta de un sistema de Historia Electrónica de Salud. [en línea]. Bogotá, 2013. [Citado en el 16 de junio de 2019]. 87 p. Disponible en: <https://consultorsalud.com/wp-content/uploads/2014/10/interoperabilidad-proyecto-esalud.pdf>

------. Políticas de Uso y Privacidad del Portal WEB SISPRO. [en línea]. Consultado en el 03 de noviembre de 2019. 2 p. Disponible en:
https://www.minsalud.gov.co/Documents/Ministerio/Terminos%20y%20Condiciones%20de%20uso%20del%20portal%20web_Octubre%202012x.pdf

------. Términos y condiciones de uso de Mi Seguridad Social. [en línea]. Consultado en el 03 de noviembre de 2019. 5 p. Disponible en:
<https://miseguridadsocial.gov.co/Registro/ValidacionDatosBasicos/DownloadFileTerminosCondiciones?Length=4>

------. Guía Metodológica para Registros, Observatorios, Sistemas de Seguimiento y Salas Situacionales Nacionales en Salud ROSS. Bogotá, 2015, [Citado en el 3 de mayo de 2019]. 132 p. Disponible en:
https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VS/ED/GCFI/ROSS_001.11.2013.pdf

------. Sistema de Evaluación del Desempeño del Sistema de Salud bajo Criterios OCDE COLOMBIA. Guía Metodológica. Bogotá, 2016, [Citado en el 3 de mayo de 2019]. 69 p. Disponible en:
<https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VS/ED/GCFI/guia-ross-ocde.pdf>

------. Política de participación social en salud PPSS. Resolución 2063 de 2017. Bogotá, 2019. [Citado en el 4 de agosto de 2019]. 45 p. Disponible en:
<https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/GT/politica-ppss-resolucion-2063-de-2017-cartilla.pdf>

Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC]. Guía para el uso y aprovechamiento de Datos Abiertos en Colombia, [Citado en el 3 de mayo de 2019]. 37 p. Disponible en: http://gobiernodigital.gov.co/623/articles-9407_guia_datos.pdf

MOLINA BULLA, Carlos Iván. Participación, políticas públicas, discapacidad mental/psicosocial y estigma: barreras y retos. [en línea]. En: Perspectivas em Políticas Públicas, 2018, vol. 11, no. 21. [Citado en el 30 de julio de 2019]. 173-200 p. Disponible en: <http://revista.uemg.br/index.php/revistappp/article/view/2891>

MONCADA ZAPATA, Juan Carlos. Siete aspectos legales en torno a la relación compliance y tratamiento de datos personales. [diapositivas]. Colombia: VII Congreso Internacional de Protección de Datos Personales, 2019. 26 p.

O'CONNOR, Siobhan, et. al. Understanding factors affecting patient and public engagement and recruitment to digital health interventions: a systematic review of qualitative studies. [en línea]. En: BMC Medical Informatics and Decision Making, 2016, vol. 16, no. 120. [Citado en el 24 de julio de 2019.] 1-15 p. Disponible en: <https://doi.org/10.1186/s12911-016-0359-3>

ORDUÑA ORTEGÓN, Yeimi Pilar. Avances en la construcción de un sistema de información en salud en Colombia. [en línea]. En: Cienc Tecnol Salud Vis Ocul, 2014, vol. 12, no. 2. [Citado en el 2 de noviembre de 2019]. 73-86 p. Disponible en: <https://doi.org/10.19052/sv.3297>

OSMA PERALTA, Sarah. 2018. The Role of search engines in Colombia after the Muebles Caqueta vs. Google Inc decision. [en línea]. En: Revista La Propiedad Inmaterial, 2018, no. 26. [Citado en el 10 de noviembre de 2019]. 143-169 p. Disponible en: <https://doi.org/10.18601/16571959.n26.06>

PRICE, William Nicholson. Risk and Resilience in Health Data Infrastructure. [en línea]. En: Colo. Tech. L.J., 2017, vol. 16, no. 1. [Citado en el 8 de mayo de 2019]. 65-85 p. Disponible en: <http://dx.doi.org/10.2139/ssrn.2928997>

PRONOVOST, Peter, et. al. 2018. Procuring Interoperability: Achieving High-Quality, Connected, and Person-Centered Care. [en línea]. Washington: National Academy of Medicine. [Citado en el 3 de mayo de 2019]. 168 p. Disponible en: <https://nam.edu/procuring-interoperability-achieving-high-quality-connected-and-person-centered-care/>

TRAVIESO Juan Antonio (Comp.) Régimen jurídico de los datos personales. Argentina: Abeledo Perrot, 2014 (Tomo II).1424 p.

RAYMOND, Anjanette. Information and the Regulatory Landscape: A Growing Need to Reconsider Existing Legal Frameworks. [en línea]. En: Wash. & Lee J. Civ. Rts. & Soc. Just, 2018, vol. 24, no. 357. [Citado en el 08 de mayo de 2019]. 357-417 p. Disponible en: <https://dx.doi.org/10.2139/ssrn.3349737>

REMOLINA ANGARITA, Nelson. Tratamiento de datos personales relativos a la salud: reflexiones en torno a la incidencia de la Ley 1581 de 2012 en el sector salud. Bogotá: Universidad de los Andes, 2014, 28 p.

REMOLINA ANGARITA, Nelson. Recolección internacional de datos personales: un reto del mundo post-internet. Madrid: BOE, 2015. 420 p.

REMOLINA ANGARITA, Nelson; ÁLVAREZ ZULUAGA, Luisa Fernanda. Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability– en las transferencias internacionales de datos personales. [en línea]. Bogotá, Universidad de los Andes, 2018. [Citado en el 8 de mayo de 2019]. 1-58 p. Disponible en: <https://habeasdatacolombia.uniandes.edu.co/?p=2817>

RENDÓN GUTIÉRREZ, Iván Santiago, et al. Historias clínicas digitales desde la perspectiva colombiana: seguridad, calidad y gestión del dato. [en línea]. En: Inventum, 2018, vol. 13, no. 24, [Citado en el 3 de mayo de 2019]. 22-28 p. Disponible en: <https://doi.org/10.26620/uniminuto.inventum.13.24.2018.22-28>

SAFRAN, Charles, et. al. Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. [en línea]. En: Journal of the American Medical Informatics Association, 2007, vol. 14, no. 1. [Citado en el 23 de mayo de 2019]. 1–9 p. Disponible en: <https://doi.org/10.1197/jamia.M2273>

SUÁREZ ROZO, Luisa Fernanda, et. al. La crisis del sistema de salud colombiano: una aproximación desde la legitimidad y la regulación. [en línea]. En: Rev Gerenc Polít Salud, 2017, vol. 16, no 32. [Citado en el 18 de junio de 2019]. 34-50 p. Disponible en: <http://dx.doi.org/10.11144/javeriana.rgps16-32.cssc>

SUNRISE WINTER, Jenifer; DAVIDSON, Elizabeth. Big data governance of personal health information and challenges to contextual integrity. [en línea]. En: The Information Society, 2019, vol. 35, no. 1. [Citado en el 3 de junio de 2019]. 36-51 p. Disponible en: <https://doi.org/10.1080/01972243.2018.1542648>

UPEGUI MEJÍA, Juan Carlos. Habeas Data: Fundamentos, naturaleza, régimen. Bogotá: Universidad Externado de Colombia. 2008. 488 p.

------. Comentario a la sentencia T-020 de 2014 de la Corte Constitucional colombiana. Apuntes sobre el “tratamiento estructurado de datos personales”. [en línea]. En: Estudios en Derecho a la Información, 2017, no. 4. [Citado en el 10 de noviembre de 2019]. 93-102 p. Disponible en: <https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/11522/13407>

WASS, Sofie; VIMARLUND, Vivian; ROS, Axel. Exploring patients’ perceptions of accessing electronic health records: Innovation in healthcare. [en línea]. En: Health Informatics Journal, 2019, vol. 25, no. 1. [Citado en el 16 de junio de 2019] 203-215 p. Disponible en: <https://doi.org/10.1177/1460458217704258>

NORMATIVIDAD

Colombia. Constitución Política. Gaceta constitucional no 114, (04, julio, 1991).

Colombia. Congreso de la República. Ley 23 (18, febrero, 1981). Por la cual se dictan normas en materia de ética médica. Diario Oficial. Bogotá, D.C., 1981, no. 35.711.

Colombia. Congreso de la República. Ley 100 (23, diciembre, 1993). Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1993, no. 41.148.

Colombia. Congreso de la República. Ley 715 (21, diciembre, 2001). Por la cual se dictan normas orgánicas en materia de recursos y competencias de conformidad con los artículos 151, 288, 356 y 357 (Acto legislativo 01 de 2001) de la Constitución Política de Colombia y se dictan otras disposiciones para organizar la prestación de los servicios de educación y salud, entre otros. Diario Oficial. Bogotá, D.C., 2001, no. 44.654.

Colombia. Congreso de la República. Ley 1122 (09, enero, 2007). Por la cual se hacen algunas modificaciones en el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones. Diario Oficial, Bogotá, D.C., 2007, no. 46.506.

Colombia. Congreso de la República. Ley 1438 (19, enero, 2011). Por medio de la cual se reforma el Sistema General de Seguridad Social en Salud y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2011, no. 47.957.

Colombia. Congreso de la República. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012, no. 48.587.

Colombia. Congreso de la República. Ley 1751 (16, febrero, 2015). Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2015, no. 49.427.

Colombia. Congreso de la República. Ley 1753 (09, junio, 2015). Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”. Diario Oficial. Bogotá, D.C., 2015, no. 49.538.

Colombia. Congreso de la República. Ley 1755 (30, junio, 2015). Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Diario Oficial. Bogotá, D.C., 2015, no. 49.559.

Colombia. Congreso de la República. Ley 1955 (25, mayo, 2019). Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”. Diario Oficial. Bogotá, D.C., 2019, no. 50.964.

Colombia. Congreso de la República. Proyecto de ley número 233 de 2019 en Senado. Por medio del cual se racionalizan trámites en el sector salud, a través de la creación de la Historia Clínica Electrónica Única y se dictan otras disposiciones.

Colombia. Presidencia de la Republica. Decreto 3380 (30, noviembre, 1981). Por el cual se reglamenta la Ley 23 de 1981. Diario Oficial. Bogotá, D.C., 1981, no. 35914.

Colombia. Presidencia de la Republica. Decreto 1074 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Diario Oficial. Bogotá, D.C., 2015, no. 49.523.

Colombia. Presidencia de la Republica. Decreto 1078 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Diario Oficial. Bogotá, D.C., 2015, no 49.523.

Colombia. Presidencia de la Republica. Decreto 780 (06, mayo, 2016). Por medio del cual se expide el Decreto Único Reglamentario del Sector Salud y Protección Social. Diario Oficial. Bogotá, D.C., 2016, no. 49.865.

Colombia. Presidencia de la Republica. Decreto 1413 (25, agosto, 2017). Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales. Diario Oficial. Bogotá, D.C., 2017, no. 50.336.

Colombia. Ministerio de las Tecnologías de la Información y las Comunicaciones. Decreto 2257 (29, diciembre, 2017). Por el cual se otorga una autorización. Diario Oficial. Bogotá, D.C., 2017, no. 50.461.

Colombia. Ministerio de las Tecnologías de la Información y las Comunicaciones. Resolución 202 (08, marzo, 2010). Por la cual se expide el glosario de definiciones conforme a lo ordenado por el inciso segundo del artículo 6 de la Ley 1341 de 2009. Diario Oficial. Bogotá, D.C., 2010, no. 47.656.

Colombia. Ministerio de Salud. Resolución 8430 (04, octubre, 1993). Por la cual se establecen las normas científicas, técnicas y administrativas para la investigación en salud. Bogotá, D.C., 1993

Colombia. Ministerio de Salud. Resolución 1995 (08, julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Diario Oficial. Bogotá, D.C., 1999, no. 43.655.

Colombia. Ministerio de salud y Protección Social. Resolución 1281 (11, abril, 2014). Por la cual se definen lineamientos para integrar la información generada por el Observatorio Nacional de Salud. Diario Oficial. Bogotá, D.C., 2014, no. 49.125.

Colombia. Ministerio de salud y Protección Social. Resolución 839 (23, marzo, 2017). Por la cual se modifica la Resolución 1995 de 1999 y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2017, no. 50.185.

Colombia. Superintendencia de Industria y Comercio y Agencia Nacional de Defensa Jurídica del Estado. Circular Externa 04 (05, septiembre, 2019). Tratamiento de datos personales en sistemas de información interoperables

JURISPRUDENCIA

Colombia. Corte Constitucional, Sentencia C-313, mayo 29 de 2014. M.P. Gabriel Eduardo Mendoza Martelo.

-----, Sentencia C-748, octubre 06 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

Colombia. Corte Suprema de Justicia, Sala de Casación Civil, Sentencia, Rad. 11001-3103-018-1999-00533-01. noviembre 17 de 2011. M.P. William Namén Vargas

-----, Sentencia, Rad. SC5641. Diciembre 14 de 2018. M.P. Margarita Cabello Blanco

Colombia. Ministerio de comercio, industria y turismo, Superintendencia de Industria y Comercio [SIC]. Resolución 83882 del 15 de noviembre de 2018.

-----, Resolución 61062 del 24 de agosto de 2018

SOFT LAW Y OTRAS PUBLICACIONES

Consejo Nacional de Política Económica y Social. Documento CONPES 3920/2018

Ministerio de Salud y Protección Social [MINSALUD]. Concepto 201811600757601/2018. 4 p.

The Global Digital Health Partnership [GDHP]. Improving health insights. [en línea]. En: GDHP Whitepapers, 2019. [Citado en el 16 de junio de 2019]. 62 p. Disponible en: https://www.gdhp.org/media-hub/news_feed/gdhp-reports

Organización para la Cooperación y el Desarrollo Económico [OCDE]. Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges. Paris, OECD Publishing, 2013a. [Citado en el 3 de mayo de 2019]. 180 p. Disponible en: <https://doi.org/10.1787/9789264193505-en>.

- . The OECD privacy framework. [en línea]. 2013b. [Citado en el 18 de mayo de 2019]. 154 p. Disponible en: <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>
- . Roadmap for the accession of Colombia to the OECD Convention. [en línea]. 2013c. [Consultado en el 18 de mayo de 2019]. 21 p. Disponible en: [http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=c\(2013\)110/final&doclanguage=en](http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=c(2013)110/final&doclanguage=en)
- . Health Data Governance: Privacy, Monitoring and Research, Paris, 2015a, [Citado en el 3 de mayo de 2019]. 200 p. Disponible en: <https://doi.org/10.1787/9789264244566-en>
- . OECD Reviews of Health Systems: Colombia 2016. [en línea]. Paris: OECD Publishing, 2015b. [Citado en el 18 de mayo de 2019]. 128 p. Disponible en: <https://doi.org/10.1787/9789264248908-en>
- . Evaluación de Impacto del Gobierno Digital en Colombia: Hacia una Nueva Metodología, Paris, 2017a. [Citado en el 3 de mayo de 2019]. 244 p. Disponible en: <https://doi.org/10.1787/9789264284272-es>.
- . New Health Technologies: Managing Access, Value and Sustainability. [en línea]. Paris, 2017b. [Citado en el 15 de mayo de 2019]. 228 p. Disponible en: <https://doi.org/10.1787/9789264266438-en>
- . Recommendation of the OECD Council on Health Data Governance. [en línea]. Paris, Health Ministerial Meeting, 2017c. [Citado en el 10 de mayo de 2019]. 16 p. Disponible en: <https://www.oecd.org/health/health-systems/health-data-governance.htm>
- . Revisión del Gobierno Digital en Colombia: Hacia un Sector Público Impulsado por el Ciudadano, Paris, 2018. [Citado en el 3 de noviembre de 2019]. 136 p. Disponible en: <https://doi.org/10.1787/9789264292147-es>
- . How's Life in the Digital Age?: Opportunities and Risks of the Digital Transformation for People's Well-being. [en línea]. Paris, OECD Publishing, 2019. [Citado en el 11 de junio de 2019]. 172 p. Disponible en: <https://doi.org/10.1787/9789264311800-3-en>
- Organización Mundial de la Salud [OMS], Organización para la Cooperación y el Desarrollo Económico [OCDE], El Banco Mundial. Delivering Quality Health Services: A Global Imperative for universal health coverage. [en línea]. Ginebra, 2018. [Citado en el 20 de mayo de 2019]. 96 p. Disponible en: <https://doi.org/10.1787/9789264300309-en>
- Organización Mundial de la Salud [OMS]. Políticas públicas para la salud pública. En: Informe sobre la salud en el mundo 2008: La atención primaria de salud, más necesaria que

nunca, Ginebra, 2008. [Citado en el 3 de mayo de 2019]. 125 p. Disponible en: https://www.who.int/whr/2008/08_report_es.pdf

------. Global diffusion of eHealth: making universal health coverage achievable. Report of the third global survey on eHealth, Ginebra, 2016, [en línea] 154 p. Disponible en: https://www.who.int/goe/publications/global_diffusion/en/

------. Perfil de Colombia en el uso de eHealth [en línea]. En: Atlas of eHealth country profiles 2015: The use of eHealth in support of universal health coverage Based on the findings of the 2015 global survey on eHealth. 2016. [Citado en el 3 de mayo de 2019]. 3 p. Disponible en: <https://www.who.int/goe/publications/atlas/2015/col.pdf?ua=1>

------. WHA71.7. (2018): Salud digital (Punto 12.4)

Organización Panamericana de la Salud [OPS]. Registros médicos electrónicos en América Latina y el Caribe: Análisis sobre la situación actual y recomendaciones para la Región. Washington, 2016, [Citado en el 3 de mayo de 2019]. 32 p. Disponible en: <http://www.paho.org/relacsis/index.php/biblioteca-usuarios/biblioteca-de-publicaciones/item/572-publicacion-registros-medicos-electronicos-en-america-latina-y-el-caribe>

Superintendencia de Industria y Comercio [SIC]. Concepto 17644871/2017. 12 p.

------. Guía para la implementación del principio de responsabilidad demostrada (Accountability). [en línea] Bogotá, 2015, [Citado en el 10 de mayo de 2019]. 26 p. Disponible en: <http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>