Revista de Bioética y Derecho
Perspectivas Bioéticas
www.bioeticayderecho.ub.edu - ISSN 1886-5887

DOSSIER CUESTIONES BIOÉTICAS DE LA PANDEMIA COVID-19

El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia

The right to personal data protection, digital technologies and the pandemic for COVID-19 in Colombia

El dret a la protecció de dades personals, tecnologies digitals i pandèmia per COVID-19 a Colòmbia

ANA GÓMEZ-CÓRDOBA, SINAY ARÉVALO-LEAL, DIANA BERNAL-CAMARGO, DANIELA ROSERO DE LOS RÍOS *

* Ana Gómez-Córdoba. Profesora Titular, grupo de investigación en Educación Médica y en Ciencias de la Salud, Escuela de Medicina y Ciencias de la Salud, Universidad del Rosario (Colombia). Email: anai.gomez@urosario.edu.co.

Sinay Arévalo-Leal. Grupo de investigación en Educación Médica y en Ciencias de la Salud, Universidad del Rosario, Bogotá (Colombia). Email: jose.arevalo@urosario.edu.co.

Diana Bernal-Camargo. Grupo de investigación en Educación Médica y en Ciencias de la Salud, Universidad del Rosario, Bogotá (Colombia). Email: diana.bernalc@urosario.edu.co.

Daniela Rosero de los Ríos. Médica general Universidad del Rosario, Cruz Roja de Colombia. Email: danielaroserodelosrios@gmail.com.

Resumen

La pandemia COVID-19 ha generado impactos sociales y políticos adicionales a los estrictamente sanitarios, llevando de un aparte a que los países, en el contexto de los estados de emergencia decretados, limiten de manera temporal algunos derechos y libertades civiles, para preservar la vida y salud de los ciudadanos; y de otra parte, han acelerado la transformación digital con el desarrollo y uso de herramientas tecnológicas para complementar las medidas de salud pública. Diversos organismos internacionales han expresado su preocupación respecto a la vulneración del derecho a la protección de datos personales en este nuevo escenario, e incluso han propuesto lineamientos éticos a tener en cuenta. En este artículo se analizarán las medidas que han sido implementadas en Colombia con ocasión de la COVID-19, desde la perspectiva del marco jurídico del derecho a la protección de datos personales vigente, y como los principios y derechos que lo componen, pueden ser reinterpretados a la luz de estas nuevas recomendaciones éticas.

Palabras clave: COVID-19; derecho a la protección de datos personales; principios éticos; derechos humanos; nuevas tecnologías; vigilancia epidemiológica.

Abstract

COVID-19 pandemic has generated additional social and political impacts beyond those strictly related to health, leading countries to, within the context of declared states of emergency, temporarily limit some civil rights and liberties in order to preserve their citizen's life and health. On the other hand, it has accelerated the digital transformation with the development and use of technological tools to complement public health measures. Several international organizations have voiced their concern about the violation of the right to personal data protection in this new scenario and have even proposed ethical guidelines to be taken into account. This article will analyses the measures that have been implemented in Colombia during COVID-19 pandemic, from the actual perspective of the legal framework of the right to personal data protection, and how its principles and rights may be reinterpreted in the light of these new ethical recommendations.

Keywords: COVID-19; right to personal data protection; ethical principles; human rights; new technologies; epidemiological surveillance.

Resum

La pandèmia COVID-19 ha generat impactes socials i polítics addicionals als estrictament sanitaris, portant d'un a part al fet que els països, en el context dels estats d'emergència decretats, limitin de manera temporal alguns drets i llibertats civils, per preservar la vida i salut dels ciutadans; i d'una altra banda, accelerant la transformació digital amb el desenvolupament i l'ús d'eines tecnològiques per complementar les mesures de salut pública. Diversos organismes internacionals han expressat la seva preocupació pel que fa a la vulneració del dret a la protecció de dades personals en aquest nou escenari, i fins i tot han proposat directrius ètiques a tenir en compte. En aquest article s'analitzaran les mesures que han estat implementades a Colòmbia amb motiu de la COVID-19, des de la perspectiva del marc jurídic del dret a la protecció de dades personals vigent, i com els principis i drets que el componen, poden ser reinterpretats a la llum d'aquestes noves recomanacions ètiques.

Paraules clau: COVID-19; dret a la protecció de dades personals; principis ètics; drets humans; noves tecnologies; vigilància epidemiològica.

1. Introducción

La declaración de la pandemia por SARS-COV 2, denominada COVID-19, ha llevado a que casi todos los países empezaran a tomar diversos tipos de medidas de forma progresiva, con la finalidad de contener la propagación, proteger la salud pública y la vida de las personas. Estas acciones de una u otra forma han limitado derechos y libertades fundamentales, a saber: la privacidad y protección de datos personales, libre circulación, libertad de expresión, libertad religiosa, reunión y manifestación, recreación, trabajo, salud, entre otros. De todos estos nos preocupa especialmente el derecho a la protección de datos personales, debido al tipo de información requerida para la implementación de los sistemas de vigilancia epidemiológica y de control de la diseminación de la enfermedad.

Sin embargo, a pesar de la restricción de libertades, debe señalarse, que acorde con los Principios de Siracusa "ningún Estado, ni siquiera en situaciones de excepción que amenacen la vida de la nación, podrá suspender las garantías contenidas en el Pacto de Derechos humanos."[1] (UN Commission on Human Rights, 1984; Silva & Smith, 2015).

En este escenario de incertidumbre y riesgo, los Estados han hecho uso de sus poderes excepcionales de intervención, sin que necesariamente medie un control político, ni se informe adecuadamente a la ciudadanía, ni se garantice su carácter temporal, o se proteja el núcleo fundamental de estos derechos, lo que incide en la falta de confianza y seguridad jurídica de los ciudadanos (Blofield, Hoffmann & Llanos, 2020).

Las epidemias han estado presentes a lo largo de la historia de la humanidad, y se han instaurado medidas para prevenir, tratar, y controlar su propagación con las herramientas disponibles en su momento. Esta pandemia es única en diversos aspectos: de una parte es altamente contagiosa, no se cuenta con una vacuna o un tratamiento efectivo, los portadores asintomáticos pueden transmitir la enfermedad, e hizo evidente que los países no cuentan con políticas claras y efectivas de salud pública, y menos para el caso de catástrofes o emergencias; y de otra parte, se da en un nuevo contexto caracterizado por los siguientes hechos: existe un entendimiento desigual por parte de las empresas privadas, los gobiernos, y los ciudadanos del

1 Acorde con los Principios de Siracusa, esta limitación aplica especialmente con respecto a: "el derecho a la vida; a no ser sometido a torturas, ni a penas o tratos crueles, inhumanos o degradantes; a no ser sometido sin libre consentimiento a experimentos médicos o científicos; a no ser sometido a la esclavitud ni a servidumbre no voluntaria; el derecho a no ser encarcelado por no poder cumplir una obligación contractual; el derecho a no ser condenado a una pena más grave en virtud de una legislación penal retroactiva; el derecho a ser reconocido como una persona ante la ley; y el derecho a la libertad de pensamiento, de conciencia y de religión. Estos derechos no admiten derogación en ninguna condición, aun cuando se afirme que su propósito sea defender la vida de la nación." (UN Commission on Human Rights, 1984).

valor de los datos, los países tienen desarrollos jurídicos que buscan garantizar el derecho a la protección de los datos personales, se cuenta con nuevas tecnologías informáticas que permiten obtener, cruzar y analizar grandes volúmenes de datos, a lo que se suma que en los últimos años ha habido una explosión del mundo digital y del e-comercio, el crecimiento de la telefonía móvil (aunque de manera desigual en distintos países y grupos poblacionales). Es común que las personas usen cotidianamente diversas plataformas como Facebook, o Google, y miles de *apps* (*Whatsapp*, *Waze*, etc.), que tienen en común la captura y almacenamiento de diversos tipos de datos de las personas.

Es decir, tenemos una amenaza tangible para la vida humana, necesitamos datos para conjurarla y contamos con los medios idóneos para hacerlo. Esta es la razón por la que gobiernos nacionales y locales como los de Singapur, Taiwán, España, Noruega, Inglaterra, Corea del Sur, India y también Colombia, emplearon diversas estrategias digitales, que complementan los instrumentos tradicionales de vigilancia epidemiológica para la detección de casos, el rastreo de contactos, corroborar el confinamiento, documentar los lugares donde las personas han estado, determinar los sitios y momentos de mayor afluencia, para así poder tomar las medidas que interrumpan el contagio. También se han usado para comunicar y educar a la ciudadanía o para hacer atención a través de tele-presencia.

Las estrategias incluyen diversas *apps*, el uso de dispositivos móviles, la medición de temperatura en lugares públicos asociada o no al reconocimiento facial, la implementación de "pasaportes inmunológicos" para hacer turismo, conseguir un empleo y hacer perfilamiento individual (*The state in the time of COVID*-19, 2020; Voo, Clapham & Tam, 2020). En Colombia, el gobierno nacional lanzó *Coronapp*, en la que más de 40.000 colombianos voluntariamente han ingresado sus datos de salud (MinTic, 2020)[2], así como otros aplicativos desarrollados por los gobiernos locales o incluso por empresas privadas.

Sin embargo, estas innovaciones han generado nuevas preocupaciones sobre la vigilancia y la privacidad de los ciudadanos, y han supuesto una tensión entre el derecho a la salud colectiva y los derechos individuales. Lamentablemente estas estrategias no siempre se contextualizan dentro de un régimen de protección de datos personales robusto, ni de instrumentos jurídicos que garanticen que en su desarrollo e implementación se protejan los derechos de las personas, se obtengan únicamente datos realmente necesarios, se evalúe el impacto en la salud humana que justifique las restricciones de libertades, o se garantice que la información obtenida no será

2 Esta aplicación ha contado con el acompañamiento de la Superintendencia de Industria y Comercio, SIC, en su rol asesor en materia de *habeas data* en Colombia.

empleada a largo plazo con otros fines estatales o privados (*World Health Organization*, 2020). Algunos de los principios del derecho a la protección de datos personales son de difícil cumplimiento en el mundo digital, como es el caso de la supresión o el almacenamiento por tiempo limitado y que cada vez es más difícil garantizar el anonimato debido a la posibilidad del cruce de datos. Ante esta realidad, diferentes organismos y entidades, como la Organización Mundial de la Salud, han propuesto una serie de principios para garantizar la transparencia y confianza por parte de la sociedad respecto al tratamiento de datos personales y evitar afectaciones a sus derechos.

Este artículo pretende hacer un análisis de las medidas del gobierno colombiano para el control de la pandemia por COVID-19 desde la perspectiva del marco jurídico vigente del derecho a la protección de datos personales y de los principios y derechos asociados que lo fundamentan, así como de los necesarios ajustes requeridos, conforme a los retos que ofrece la pandemia. Para cumplir con este objetivo nos planteamos una serie de interrogantes como hilo conductor de la reflexión.

2. ¿Cómo se entiende el derecho a la protección de datos personales y su relación con el derecho a la intimidad?

El derecho a la protección de datos personales es un derecho fundamental que se puede definir como el:

> *"conjunto de facultades que le permiten a la persona tener control sobre el tratamiento de sus propios datos, bien sea que estos se encuentren en soportes manuales o automatizados o que hagan referencia a su vida íntima o privada, e imponer a terceros que actúen o se abstengan de realizar acciones respecto de ellos."* (Seoane, 2002)

Este derecho está íntimamente relacionado con la dignidad y con los derechos a la intimidad, al buen nombre, al acceso a la información, a la libertad, y a la autodeterminación informática y libertad informativa, entre otros. El consentimiento previo, expreso, informado, inequívoco y comprobable, que da el titular para el tratamiento legítimo de sus datos, es el eje central del control que este puede ejercer sobre ellos.

3. ¿Bajo qué condiciones pueden los Estados restringir el derecho a la protección de datos personales?

Diversos instrumentos de *softlaw* y las reglamentaciones de los diferentes países contemplan una serie de principios, derechos y deberes relacionados con el derecho a la protección de datos personales, de las que se destaca la necesidad de contar con el consentimiento del titular para el tratamiento de los datos para una finalidad específica. No obstante, también prevén circunstancias extraordinarias en las que puede obviarse este requisito, como es el caso de las emergencias sanitarias. Sin embargo, estas medidas deben acompañarse de una reflexión ética que las sustenten, que sean comunicadas al momento de tomar estas decisiones, de tal forma que se eviten daños a grupos vulnerables, la sociedad pierda la confianza y no se logre la coordinación requerida entre los actores clave (Esquivel-Guadarrama, 2020).

Algunas de estos documentos son, entre otros: las *Pautas de la OMS sobre la ética en la vigilancia de la salud pública* (2017); el documento de *Orientación ética sobre cuestiones planteadas por la pandemia del nuevo coronavirus COVID-19* (OPS, 2020); el *Documento sobre consideraciones éticas para la orientación del uso de tecnologías digitales para el rastreo de contactos (contact tracking apps) para COVID-19* (OMS, 2020); *Resolución 01 de 2020* de la Comisión Interamericana de Derechos Humanos–CIDH (2020), la *Declaración sobre epidemias y pandemias* de la Asociación Médica Mundial (2017); la *Declaración conjunta sobre el derecho a la protección de datos en el contexto de la pandemia de COVID-19* emitida por la Presidenta de la Comisión de la Convención 108 y el Comisionado de Protección de Datos del Consejo de Europa (2020); el informe con recomendaciones del Comité Internacional de Bioética de Unesco sobre *Big Data y Salud* (2017), el *Convenio de Biomedicina y Derechos Humanos* del Consejo de Europa (1997).[3]

Las pautas 10, 11 y 12 del documento *Pautas de la OMS sobre la ética en la vigilancia de la salud pública*[4], en consonancia con los otros instrumentos referidos, reconocen la injerencia al derecho a la privacidad cuando se está frente a la necesidad de proteger un interés público

3 Estas normativas son de interés en el marco jurídico colombiano como normas de *softlaw* toda vez que el tratamiento de datos con ocasión de la pandemia por COVID-19 puede conllevar la transferencia internacional de datos.

4 Pauta 10: Los gobiernos y otras entidades que tienen datos de vigilancia en su poder deben mantener debidamente resguardados los datos que permiten identificar a las personas. Pauta 11: En ciertas circunstancias, se justifica la recolección de nombres o datos que permitan identificar a las personas. Pauta 12: Las personas tienen la obligación de contribuir con la vigilancia cuando se requieren conjuntos de datos fiables, válidos y completos y se cuente con la debida protección. En estas circunstancias, el consentimiento informado no es un requisito ético.

señalando que "si bien el consentimiento informado no es obligatorio en el contexto de vigilancia en salud pública, el tratamiento de los datos personales debe realizarse teniendo en cuenta las excepciones y condiciones que por ley le aplique" (OMS, 2017). Sin embargo, hacen un llamado especial al reconocimiento de los daños que se puedan generar con ocasión de la vigilancia en salud pública a partir del tratamiento de datos personales, y enfatizan no sólo en los deberes de privacidad y confidencialidad, sino en especial en la seguridad entendida como las diferentes "medidas operativas y tecnológicas para proteger los datos personales" (OMS, 2017).

El documento *Orientación ética sobre cuestiones planteadas por la pandemia del nuevo coronavirus (COVID-19)* se refiere a la rigurosidad del manejo de la información, la confidencialidad en la medida de lo posible y la transparencia de esta (OMS, 2020).

Por su parte, el documento sobre *Consideraciones éticas para la orientación del uso de tecnologías digitales para el rastreo de contactos (contact tracking apps) para COVID-19* sugiere un catálogo de 17 principios dirigido a gobiernos, instituciones de salud pública, actores no estatales (organizaciones no gubernamentales, organizaciones benéficas, fundaciones) y compañías con el fin de orientar sobre el uso ético y apropiado de estas tecnologías (OMS, 2020).[5]

En consonancia con estas orientaciones, la Resolución 01 de 2020 de la CIDH reitera que el manejo de los datos personales debe hacerse bajo unos principios, con el fin de evitar vulnerar los derechos de los ciudadanos. Concluye la CIDH diciendo que, por ello, estas medidas adoptadas en el marco de la pandemia deben estar limitadas en el tiempo, y que las leyes de protección de datos implementadas por cada país deben encontrarse apegadas a estándares y normas internacionales en materia de derechos humanos (CIDH, 2020).

Ante la necesidad de contar con información para el manejo adecuado de la pandemia, es admisible el tratamiento de datos personales sin el consentimiento de los titulares. Sin embargo, este tratamiento debe ser justificado, necesario, proporcional, razonable y eficaz como medida para contener la propagación, y se debe garantizar la seguridad en el tratamiento de los datos. El poder excepcional del Estado debe estar limitado por el respeto al núcleo esencial de los derechos fundamentales y la aplicación de los principios generales para el manejo de emergencias sanitarias, como son los de: confianza, transparencia, participación y planificación.

En este sentido, en los diferentes instrumentos se insta a los Estados a establecer medidas adecuadas y específicas con el fin de proteger los derechos y libertades de las personas (IBC, 2017), con un especial llamado a garantizar la temporalidad de los datos, la no identificación

5 En nuestro parecer al comparar los principios aquí enunciados, respecto a los que se describen en otros documentos, este es uno de los más completos razón por la cual la utilizaremos posteriormente en nuestro análisis como línea de base.

directa o la re-identificación (Pierucci & Walter, 2020) y el deber de brindar la información sobre la recolección de los datos de manera transparente (OMS, 2017; OMS, 2020).

4. ¿Qué contempla el régimen jurídico colombiano en materia de protección de datos personales aplicable al contexto de COVID-19?

El marco jurídico colombiano en el cual se sustenta el derecho a la protección de datos personales, conocido también como derecho al *habeas data*, está conformado por la Constitución Política de Colombia de 1991, un amplio desarrollo jurisprudencial de las altas Cortes, la Ley Estatutaria 1581 de 2012 (LEPDP) "por la cual se dictan disposiciones generales para la protección de datos personales", y en el Decreto 1377 de 2013, que reglamenta parcialmente esta Ley.

Este régimen es de tipo híbrido, que cuenta, por una parte, con una Ley Estatutaria en la que se enuncian una serie de principios generales que determinan el tratamiento de los datos personales, los derechos de los titulares y las obligaciones de los responsables y encargados del tratamiento, así como los actores e instituciones responsables del control; y, por otra, con el desarrollo posterior de reglamentación sectorial. Lamentablemente, en el ámbito de la salud, la reglamentación complementaria es incompleta y en su mayoría precede a la Ley estatutaria.

Conforme a esta normativa, se entiende por dato personal, "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables" (Ley 1581, 2012, art. 3., lit. c). Los principios enunciados en la LEPDP son los de: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad (Ley 1581, 2012, art. 4). A estos principios se adicionan los principios rectores derivados directamente de la Constitución. Son derechos de los titulares en relación con sus datos personales: decidir si desea o no ser informado, oposición, acceso, rectificación, y cancelación (Ley 1581, 2012).

En Colombia, al igual que en otros países, está prohibido el tratamiento de los datos personales sensibles –dentro de estos, los de salud –, excepto en determinadas circunstancias, como son: cuando se cuenta con la autorización explícita del titular, cuando el tratamiento tiene como objeto la guarda del interés vital del titular y este se encuentra incapacitado para dar su consentimiento (aunque deberá solicitarse a su representante legal) y cuando hay fines históricos, científicos, o epidemiológicos (Ley 1581, 2012). Estas excepciones se enuncian también en el art. 6 del Decreto reglamentario, que señala que se permite el tratamiento de los datos sin la autorización del titular o quien lo represente en determinadas circunstancias:

> *"a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; b) Datos de naturaleza pública; c) Casos de urgencia médica o sanitaria; d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; e) Datos relacionados con el Registro Civil de las Personas."* (Ley 1581, 2012, art.10)

Se contempla una figura de control de la autoridad de protección de datos, la cual es ejercida por la Superintendencia de Industria y Comercio por medio de la Delegatura para la Protección de Datos Personales. Esta tiene como objetivo "garantizar que en el Tratamiento de los datos personales se respeten los principios, derechos, garantías y procedimientos previstos" (Ley 1581, 2012.art. 19).

En referencia a la autorización para el tratamiento de datos personales sensibles señala que se deben cumplir las siguientes obligaciones:

> *"1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento. 2. Informar al titular de forma explícita y previa, además de 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. Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles."* (Decreto 1377, 2013, art. 6)

En relación con estas excepciones la Corte Constitucional se ha pronunciado señalando en la Sentencia C-748 de 2011 que esta excepción es aplicable:

> *"sólo en los casos en que dada la situación concreta de urgencia, 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."* (Corte Constitucional, 2012)

Y adiciona que "el uso del dato también debe sujetarse a todos los principios y limitaciones consagrados en la Ley. Por el contrario, jamás podría interpretarse como una autorización abierta para que se acceda a datos personales sin consentimiento de su titular" (Corte Constitucional, 2012).

Sumarizando, Colombia cuenta con un régimen jurídico cuyos principios permiten la protección efectiva de los datos personales y que puede ser extrapolable y adaptado a las

circunstancias de la pandemia. También que la excepción por urgencia médica o sanitaria[6] no puede ser aplicada de forma indiscriminada para eludir la necesidad de consentimiento del titular de los datos, y que resulta especialmente problemático para la instauración de medidas de control en el contexto de la pandemia que no pueda condicionarse ninguna actividad a la entrega de datos personales sensibles, como son los de salud.

Colombia declaró el estado de emergencia sanitaria en el territorio nacional mediante la Resolución 385 del 12 de marzo, expedida por el Ministerio de Salud y Protección Social (MinSalud) (2020), y declaró el Estado de Emergencia Económica, Social y Ecológica en todo el territorio Nacional mediante el Decreto Presidencial 417 de 2020, a partir de la cual se han adoptado distintas medidas que se clasifican en tres fuentes "medidas sanitarias y de emergencia sanitaria, medidas de emergencia social, económica y ecológica y medidas de orden público y otras de carácter ordinario" (Ministerio de Salud y Protección, 2020).

Cuando se analizan las medidas sanitarias implementadas en Colombia y se compara con el marco jurídico vigente, existen dudas razonables sobre la garantía al derecho a la protección de datos personales, como se expondrá a continuación.

La Superintendencia de Industria y Comercio (SIC), mediante circular externa 001 dirigida a los operadores de telefonía móvil y a la Asociación de la Industria móvil, los autoriza para suministrar información al Departamento Nacional de Planeación (DNP) y demás entidades estatales que la requieran para "atender, prevenir, tratar o controlar la propagación del COVID-19 Coronavirus y mitigar sus efectos", sustentados en el artículo 10 de la Ley 1581 de 2012, que señala que no es necesaria la autorización para el tratamiento de datos personales en situaciones de urgencia médica o sanitaria, y en el literal b del artículo 13 que señala que los datos personales pueden ser entregados a las entidades públicas administrativas en ejercicio de sus funciones legales (Circular 001, 2020).

Consideramos, al igual que otros actores sociales en el país, que esta circular es muy amplia, no define las finalidades de uso, la información que será recolectada, el límite de tiempo de almacenamiento no limita el acceso a datos registrados durante la pandemia, no adapta los principios del régimen de protección de datos nacional a la situación específica, ni tiene en cuenta los lineamientos que ya habían sido emitidos por instancias internacionales como la OMS. Adicionalmente, la carencia de un sistema autónomo, independiente y robusto de protección de datos personales en salud remarca estas problemáticas.

6 La legislación colombiana se refiere literalmente a la excepción de consentimiento informado para el tratamiento de datos en caso de "urgencia médica o sanitaria".

Mediante Circular Externa 002 del 24 de marzo de 2020 la SIC ordenó a los responsables o encargados abstenerse de recolectar o tratar datos mediante huelleros físicos o electrónicos, por el riesgo de contagio asociado. Posteriormente, de forma reactiva y posiblemente frente a la presión de distintos actores sociales, detalla en su página electrónica las medidas para el uso y recolección de los datos personales en caso de urgencia médica o sanitaria frente a la pandemia por COVID-19 y señala que se deben tomar medidas para garantizar los principios de finalidad, veracidad o calidad, acceso y circulación restringida, y seguridad[7], sin incluir el principio de transparencia. Sin embargo, consideramos se quedan cortos frente a los riesgos existentes frente a las nuevas tecnologías, a la posibilidad de cruce de datos, y a su análisis algorítmico o por inteligencia artificial.

La SIC mediante Resolución No. 12169 de 2020, suspendió desde el 1 de abril de 2020 y hasta la vigencia del Estado de Emergencia Económica, Social y Ecológica declarado por el Presidente de la República, los términos de sus actuaciones administrativas sancionatorias y disciplinarias en curso con algunas excepciones, entre ellas la garantía constitucional del *habeas data*, derechos del consumidor y las actuaciones requeridas para conjurar la crisis por COVID-19 (Resolución 12169, 2020).

MinSalud, señala que es necesario durante el tiempo de la emergencia sanitaria flexibilizar el literal g del artículo 4 de la Ley 1581 de 2012 y el literal b del artículo 32 de la Ley 527 de 1999:

> *"en el sentido de implementar plataformas digitales accesibles con estándares básicos de audio y video que permitan el diagnóstico y seguimiento del paciente, sin que sea necesario cumplir los estándares técnicos señalados en los precitados artículos. Si bien esta medida incide en la seguridad de los datos de los pacientes, se garantizan los principios y derechos de mayor valor constitucional, como lo son la vida y la salud de las personas que acuden a estas plataformas".* (Decreto 538, 2020)

También señala en el parágrafo segundo del artículo 8 que los pacientes:

> *"podrán enviar la imagen del documento firmado en el que manifieste el consentimiento informado. Cuando esto no sea posible, el profesional tratante dejará constancia en la historia clínica de la situación, de la información brindada sobre el*

7 Se señala: "(i) la finalidad para la que se deben usar los datos recolectados bajo esta excepción debe consistir en prevenir, tratar y controlar la propagación del COVID-19; (ii) se debe garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible; (iii) que se aplique el principio de acceso y circulación restringida de forma que la información deba usarse exclusivamente para prevenir o tratar el COVID-19; y (iv) que se deben adoptar las medidas de seguridad para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información." (SIC, 2020).

alcance de la atención y de la aceptación del acto asistencial por parte del paciente, de forma libre, voluntaria y consciente." (Decreto Legislativo 538, 2020, art. 8)

En nuestro concepto, a pesar de que se pretende garantizar el derecho a la salud mejorando el acceso, se expone a los pacientes a vulneraciones al derecho a la protección de datos, no se garantiza el principio básico de seguridad, no se exige que se informe los riesgos en el tratamiento de los datos bajo esta nueva modalidad, ni se garantiza la calidad misma del acto médico.

MinSalud emitió un protocolo general de bioseguridad con el fin de mitigar, controlar y realizar el adecuado manejo de la pandemia de COVID-19, para ser implementado por los empleadores, trabajadores y aseguradoras del régimen laboral (ARL), tanto públicos como privados, que requieran desarrollar sus actividades durante el periodo de la emergencia sanitaria. Se señala como deberes de los empleadores reportar los casos sospechosos y confirmados a las empresas promotoras de salud (EPS) y promover el uso por los empleados del aplicativo *Coronapp*. Como deberes de los empleados se enuncian reportar al empleador, jefe inmediato, cualquier caso de contagio en la empresa o en el núcleo familiar, así como cualquier síntoma de enfermedad respiratoria y registrar la información en el aplicativo ya mencionado (Resolución 666, 2020).

En consecuencia, el Ministerio del Trabajo (MinTrabajo) presenta unos lineamientos mínimos de carácter temporal y señala que los empleadores deben establecer canales de comunicación oportunos frente a la notificación de casos de COVID-19 ante las autoridades de salud competentes (secretarías de salud). El suministro de información debe ser oportuno y veraz y deberá implementar la ruta de notificación e incluir los datos de contacto. Las ARL deben garantizar el registro de los trabajadores con riesgo de exposición directa al COVID-19 y de aquellos con diagnóstico confirmado, según información suministrada por los empleadores y esta información debe ser disponible para las autoridades de trabajo y salud. Los trabajadores deben suministrar información clara, veraz y completa de su estado de salud (Circular 0017, 2020).

En contraste, la normatividad colombiana referente a salud y medicina del trabajo (Resolución 2346, 2007) que regula la práctica de evaluaciones médicas ocupacionales y el manejo y contenido de las historias clínicas ocupacionales, es clara en especificar que los empleadores sólo pueden conocer la existencia de una incapacidad y las medidas de acompañamiento e incorporación al trabajo, por tanto no pueden ser las áreas de recursos humanos o los jefes inmediatos quienes recaben información referente a síntomas o diagnósticos. Esta información debe estar bajo la responsabilidad de áreas de medicina del trabajo, por profesionales de la salud ocupacional y con las medidas requeridas para garantizar la privacidad y confidencialidad en el tratamiento de estos datos, a no ser que se cuente con el consentimiento

del trabajador, dado el riesgo de discriminación y estigmatización asociado. Las empresas están solicitando información de carácter sensible para determinar el riesgo de regreso al trabajo en fase de desescalada, como son los antecedentes patológicos o medicamentosos. El consentimiento en general no está precedido de información sobre los riesgos, los derechos del titular o los deberes del responsable o el encargado de la base de datos. No es un consentimiento libre, dado que hay subordinación del empleado al empleador, más aún cuando existe el temor de perder el empleo en este momento.

A nuestro juicio, todo esto es contradictorio con las indicaciones de ruta de notificación señalados en la Resolución 666 de 2020 y en la circular 0017 de 2020. Nos preguntamos ¿qué pasará cuando un empleado no desee dar su consentimiento para el tratamiento de esta información, debido a que padece un patología que puede estar asociada a estigma o discriminación posterior?, ¿se afectara su derecho al trabajo?, ¿cómo se garantiza la privacidad y confidencialidad si los responsables del tratamiento no están sujetos a secreto profesional, como sí lo están los médicos o demás profesionales en medicina del trabajo?, más aún cuando la regulación prevé que no se puede supeditar ninguna actividad al consentimiento para el tratamiento de datos personales de tipo sensible.

En Colombia no solo se ha implementado *Coronapp*. Las alcaldías de Bogotá, Cali y Medellín cuentan con plataformas y *apps* como "Bogotá Cuidadora", "Gabo" (Gobierno abierto de Bogotá), "CaliValleCorona" y "Medellín me Cuida". En el caso de la *app* "Bogotá cuidadora", incluye apartados de registros de movilidad segura, necesito apoyo, reportar estado de salud y COVID a mi alrededor. Esta *app* inicialmente tenía un carácter obligatorio, pero debido a la presión ciudadana por dudas razonables en su seguridad y eficacia, se hizo voluntaria. Posterior a la implementación de las *apps*, la SIC pidió a las alcaldías respuesta a las solicitudes planteadas en relación a si cumplían "la regulación colombiana sobre la recolección y tratamiento de datos personales y si han implementado el principio de responsabilidad demostrada (*Accountability*)." (Portafolio, 2020).

Con la apertura de distintas actividades en la fase de desescalada se enfrentan nuevos retos. En el comercio, cada empresa está decidiendo tomar distintos tipos de datos ante la ausencia de lineamientos por parte de las autoridades competentes, en aras de garantizar la salud pública en sus instalaciones y la salud de sus trabajadores: se toma y registra la temperatura corporal, se pregunta el nombre, ocupación, número de identificación personal, asegurador, dirección, número de móvil, el sitio donde ha estado anteriormente e incluso se realiza el escaneo del documento de identificación, mediando únicamente el consentimiento tácito de las personas, sin una adecuada información, o sin que el responsable del tratamiento de los datos sea idóneo para

garantizar los principios del derecho a la protección de datos personales, e incluso se condicionan otros derechos a la entrega de esta información.

5. ¿Qué prácticas generan un riesgo para los derechos humanos cuando se emplean herramientas digitales para la captura de datos personales en el contexto de la pandemia por COVID-19?

Los riesgos asociados con el uso de nuevas tecnologías para el control de la extensión de la pandemia y la afectación de derechos humanos nominados e innominados son el uso obligatorio de las aplicaciones de vigilancia epidemiológica[8], la georreferenciación[9], el escaneo de temperatura[10], el uso de los datos con finalidades distintas a las justificadas para el control de la pandemia o las consentidas por el titular, y el acceso de terceros no autorizados[11], tiempo de

8 Si bien en algunos países registrarse en este tipo de aplicaciones es opcional, en otros ha sido obligatorio descargarlas y usarlas para poder ejercer otros derechos como son los de: salud, trabajo, libre circulación, derechos del consumidor, entre otros. Esto limita no sólo los derechos anteriormente descritos sino también la autonomía y libre determinación de las personas.

9 Entendida como la identificación de la ubicación de un usuario de telefonía móvil, y la posibilidad de contacto con otros (*contact tracking*), si bien es útil para establecer posibles contagios de un caso diagnosticado, representa un riesgo al derecho a la privacidad, a la libre asociación, intimidad y privacidad familiar.

10 La temperatura es un dato de salud, que, asociado a la identificación del titular, es un dato personal sensible. La medición de la temperatura se ha instaurado como medida de control para la detección de posibles personas infectadas por COVID-19, y se puede hacer mediante cámaras termográficas y termómetros infrarrojos. Las primeras pueden ir o no acompañadas de datos biométricos como el de reconocimiento facial, y las segundas generalmente se acompañan del registro manual de datos personales. Si se trata de una cámara termográfica que no permite el reconocimiento facial, no se trataría de un dato personal, en los otros casos descritos, sí. Se supone que si una persona tiene fiebre no pude acceder a un lugar público o privado, sin embargo, los portadores asintomáticos, pueden no tener fiebre, una persona enferma puede tener un cuadro sintomático en el que este signo no esté presente y otro tipo de patologías pueden acompañarse de un aumento de la temperatura. Nos preguntamos: ¿quién es la persona idónea para tratar este dato sensible de salud?, ¿con qué grado de temperatura se puede negar el acceso?, ¿se debe reportar esta persona a las autoridades de salud?, ¿quién lo debe hacer?, ¿una persona tiene el derecho a explicar otras causas de fiebre, y cómo y quién lo valida?, ¿están preparados los encargados y responsables de estos datos para garantizar los principios que rigen su tratamiento?, ¿es justificable como parte de un protocolo en el ámbito laboral? Dada la posibilidad de falsos positivos se está estigmatizando a un grupo de personas, se puede estar vulnerando los derechos a la intimidad, a la no discriminación, a la no estigmatización, al trabajo, al aseguramiento en salud. Incluso para aquellas empresas que tratan estos datos sin estar preparados, puede convertirse en un riesgo reputacional. Esta medida requiere ser revisada para su aplicación desde su idoneidad, necesidad, proporcionalidad, eficacia y temporalidad

11 Como otras autoridades (policiales o de migración), o empresas privadas con fines comerciales. La tendencia a la "datificación de lo personal y su comercialización amplifica el uso potencial de estos datos como dispositivos de control social e intervención pública y privada" (Observatorio Bioética y Derecho, 2015, p.2). Se vulnera el derecho a la autonomía, a la intimidad, y a la seguridad personal.

conservación indefinido[12], recolección de un número mayor de datos que los necesarios[13], información parcial, incompleta, sesgada, estandarizada para el uso de las plataformas y aplicaciones[14], Implementación de aplicativos o plataformas[15], falta de garantías técnicas y procedimentales[16] y desarrollo de *apps* falsas[17].

5.1 ¿Cómo deben ser reinterpretados los principios que sustentan el tratamiento de datos personales en Colombia ante los nuevos desafíos en tiempo de pandemia?

Si bien la legislación colombiana incluye una serie de principios en materia de tratamiento de datos personales, se hace necesario ampliarlos y re-interpretarlos a las luz de pautas y orientaciones éticas internacionales afines al derecho a la protección de datos personales, que estén contextualizados en los riesgos que ya han sido evidentes y los que pueden materializarse en el futuro, de tal forma, que se intervengan o eviten, con el fin de contar con un marco regulatorio que ofrezca seguridad jurídica, proteja los derechos de las personas y genere confianza en la sociedad. A continuación, se enuncian los principios que hacen parte de la Ley de protección de datos colombiana, y los derechos de los titulares de los datos personales, y cómo estos se relacionan con las recomendaciones éticas OMS en la pandemia de COVID-19:

12 Este tipo de herramientas digitales, por diseño, conservan de forma indefinida los datos y el riesgo que sean empleados con otros fines después de la pandemia es latente. En este caso se afecta el derecho a la protección de datos, como derecho humano innominado. Sin embargo, algunos abogan que estos datos deben ser conservados de forma indefinida y anonimizados, para ser empleados en investigación o planificación de políticas de salud.

13 Sumado a la posibilidad de cruce permitan la identificación de los titulares. En este caso se vulnera el derecho a la información, la intimidad y el principio de finalidad del derecho a la protección de datos.

14 Generalmente se brinda una información genérica, en la que se indica que se atendrá a la normativa de protección de datos personales, como una formalidad que no protege realmente los derechos del titular, incumpliendo el principio de transparencia. Se vulnera el derecho a la información y los derechos de los consumidores.

15 En ellas se recolectan datos personales sin que se determine su eficacia para el control de la pandemia. Se vulnera el derecho a la protección de datos personales dado que no existiría una justificación legal para su tratamiento.

16 Estas garantías se enfocan en la confidencialidad, intimidad y seguridad en el tratamiento de los datos, haciendo más fácil el acceso por terceros no autorizados e incluso posibilita ciber-ataques.

17 Este tipo de *apps* dependen de las autoridades de salud de los Estados y que tienen como único fin la captura de datos personales que facilitan acciones delictivas.

Principios (Ley 1581, 2012)	Recomendaciones éticas OMS (2020)
Principio de legalidad en materia de tratamiento de datos[18]	Seguimiento[19]
Principio de finalidad[20]	Restricción en su uso[21] Proporcionalidad en la recolección de datos[22] Recolección mínima de datos para el logro de objetivos de salud pública
Principio de libertad[23]	Voluntariedad[24]
Principio de veracidad o calidad[25]	Evaluación y análisis[26] Precisión en los algoritmos modelos empleados
Principio de transparencia[27]	Transparencia[28] Participación de la sociedad civil[29]
Principio de acceso y circulación restringida[30]	Seguridad[31] Responsabilidad[32]

Tabla 1. Principios de la ley de protección de datos personales colombiana a la luz de las recomendaciones éticas de la OMS en la pandemia por COVID-19

18 El Tratamiento al que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
19 Después de que una persona es detectada como positiva para la infección, se pueden rastrear sus movimientos durante la infección y recuperación, así como sus posibles contactos.
20 El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
21 Prohibición de venta o uso con fines de comercio o publicidad, ni ser intercambiado con otras agencias gubernamentales como la policía o migración.
22 Justificados, adecuados para el objetivo, necesario y razonable con los fines legítimos de la salud pública. Se debe preferir, en el diseño, las medidas menos intrusivas.
23 El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
24 No puede ser obligatoria, no se puede incentivar su uso negativa o positivamente, se debe poder apagar o eliminar en cualquier momento. El reporte de infección lo puede hacer el usuario del dispositivo directamente en la aplicación, idealmente confirmado por un profesional de la salud. Una vez se confirma un contagio un profesional puede notificar a los usuarios detectados por seguimiento de proximidad previo.
25 La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
26 Tecnologías novedosas deben ser probadas antes de generalizar su uso, para garantizar su seguridad y efectividad, y evaluadas en su funcionamiento por organismos independientes.
27 En el tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del tratamiento o del Encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le concierne.
28 Las personas deben ser informadas de forma clara e inequívoca sobre el propósito de la recopilación, almacenamiento, acceso, tiempos de conservación, funcionamiento de los aplicativos, toma de decisiones automatizada, utilidad y posibilidades de error de los modelos.
29 Las medidas instauradas para la respuesta a la pandemia por COVID 19 que incluye esfuerzos en la recolección de datos debe incluir la participación libre y activa de partes interesadas como expertos en salud pública y organizaciones de la sociedad civil.
30 El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley; los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.
31 Implica cifrado de los datos personales y de salud, pruebas respecto a la penetración por parte de terceros y auditorías respecto a solicitud de datos. Optar por opciones de almacenamiento que preserve la seguridad, de ahí que muchos prefieran los modelos descentralizados que incluyen el consentimiento del titular para el tratamiento y posibilidad de retiro de los datos.
32 Contar con salvaguardas contra el abuso.

Derechos (Ley 1581, 2012)	Recomendaciones éticas OMS (2020)
Derecho a no ser informado[33]	Notificación: Los posibles contactos se informarán a través de la aplicación preservando la privacidad de la persona infectada, con los pasos a seguir, las personas deben poder escoger si desean o no ser notificadas por las autoridades de salud.
Derecho a la oposición[34]	No se encuentra principio asociado a partir de las recomendaciones éticas de la OMS.
Derecho al acceso[35]	No se encuentra principio asociado a partir de las recomendaciones éticas de la OMS.
Derecho a la rectificación[36]	No se encuentra principio asociado a partir de las recomendaciones éticas de la OMS.
Derecho a la cancelación[37]	Limitación en el tiempo[38] Retención ilimitada[39] Voluntariedad[40]

Tabla 2. Derechos de la ley de protección de datos personales colombiana a la luz de las recomendaciones éticas de la OMS en la pandemia por COVID-19

De los principios enunciados la evaluación de la seguridad de los aplicativos por organismos independientes no se encuentra de manera explícita en la reglamentación colombiana y los demás se pueden relacionar con el marco jurídico vigente para fortalecer su interpretación.

Consideramos que dada la posibilidad de falsos positivos o de sospechas diagnósticas que finalmente no sean confirmadas, es necesario que los titulares de los datos puedan exigir el derecho a la rectificación. Resulta llamativo que los documentos de la OMS no incluyen este aspecto, pero si lo hacen las directrices del comité europeo de protección de datos (Directrices 04, 2020).

33 Entendido con un derecho diferente al consentimiento, que implica la facultad del titular para para ejercer su autodeterminación informativa con el fin de recibir de forma clara, expresa e información necesaria respecto de los datos que serán objeto de tratamiento (finalidad, temporalidad, etc.) (Espiérrez, 2016).
34 Entendido como ese derecho de los titulares para ejercer control sobre sus datos personales, y en consecuencia oponerse a que el responsable realice un tratamiento de sus datos para fines diferentes a los autorizados (Murillo, 2016).
35 Entendido como el derecho que tiene el titular al acceso gratuito y conocimiento de sus datos personales que estén siendo objeto de tratamiento (INAI, 2012).
36 Comprende el derecho de toda persona para que cuando corresponda sus datos sean rectificados y actualizados de acuerdo a la información que en efecto corresponda a la realidad (Murillo, 2016).
37 Entendido como el derecho que tiene el titular de solicitar al responsable de sus datos personales la cancelación del tratamiento de estos, cuando se considere que estos no están siendo tratados conforme a los principios y derechos previstos por ley y en la constitución. La cancelación implica la supresión total o parcial de los datos personales en cualquier fuente de almacenamiento de la información (registros, archivos, bases de datos, entre otros) (INAI, 2012).
38 Las medidas de monitoreo y vigilancia deben retirarse una vez la pandemia sea controlada localmente.
39 Los datos se retienen limitado al periodo de respuesta a la pandemia, con la excepción de investigación y planeación en salud pública, pero deben agregarse y anonimizar de ser posible y solicitar el consentimiento.
40 Se debe poder eliminar la aplicación en cualquier momento.

6. ¿Qué consideraciones mínimas deben tenerse en el diseño de estos aplicativos?

La *Open Web Application Security Project* (OWASP) señala como riesgos de seguridad en las aplicaciones web que pueden exponer los datos sensibles, como los de salud, entre otros: inyección (envío de datos hostiles para ejecutar comandos no deseados); autenticación rota (compromiso de contraseñas); exposición de datos por ausencia de barreras adicionales como el cifrado en reposo o en tránsito; archivos XLM que permiten conocer los recursos internos del programa; vulnerabilidad de los controles de acceso y malas configuraciones de seguridad; redireccionamiento a sitios fraudulentos para robo de información (sitios maliciosos); uso de componentes con vulnerabilidades conocidas; insuficiente registro y monitoreo (OWASP, 2020).

En este orden de ideas se recomienda: que en el diseño exista un equipo responsable que garantice la protección de los datos; clasificar la información para identificar aquella que es sensible y protegerla selectivamente; definir controles de acceso (con usuario único y contraseñas robustas y dinámicas) para restringir acceso no autorizados; doble autenticación; protección frente a códigos maliciosos; copias de seguridad; cifrado de datos sensibles; monitorización y *logs* de auditoría; medidas de seguridad lógica (*firewall*, segmentación de red); contratos con terceros y proveedores fiables con certificaciones de alta calidad, sujetos a cláusulas de confidencialidad y desarrollo de código seguros y segregación de entornos. Muchas estas acciones son las que se emplean en el ámbito hospitalario para proteger los datos en las historias clínicas electrónicas.

6. Conclusiones y recomendaciones

La pandemia por COVID-19 debe ser entendida como una oportunidad histórica de aprendizaje para la protección de los derechos individuales y colectivos, que fortalezca la confianza de los ciudadanos en los gobiernos, a pesar de las declaraciones de estados de excepción.

No se debe fomentar en el imaginario colectivo la falsa dicotomía entre la vida y la salud pública y la protección de los derechos, en especial el de la protección de datos personales.

La restricción de derechos no puede afectar el núcleo fundamental de estos, debe ser temporal, conforme al principio de legalidad, responder a una necesidad perentoria, ser proporcional a esta, no generar discriminación, ni estigmatización (como es el caso de los pasaportes inmunológicos), no mantenerse de forma permanente, no ser arbitrarios, así como estar plenamente justificados.

La adaptación de los sistemas de protección de datos personales a los retos que imponen las medidas de salud pública en tiempos de pandemia deben salvaguardar los derechos humanos y responder a las particularidades jurídicas y culturales de cada país, de manera que nadie se vea obligado a elegir entre una respuesta eficaz para el control de la pandemia y la protección de sus derechos fundamentales. En el mundo digital algunos de ellos son de más difícil aplicación como es el caso de cancelación de los datos.

El sistema de protección de datos personales colombiano a pesar de tener un carácter general y no contar con una reglamentación sectorial para salud plenamente estructurada, permite la adaptación e interpretación de los principios y derechos a las actuales circunstancias acorde con los lineamientos éticos emanados de diferentes instrumentos de *softlaw.* Sin embargo, este ejercicio no fue hecho por las autoridades competentes, exponiendo a los ciudadanos a los riesgos enunciados en este artículo, bajo el pretexto de las excepciones por urgencia o emergencia sanitaria, incluso sin tomar en consideración los conceptos previos de la Corte Constitucional en esta materia. En adición es necesario robustecer el régimen de protección de datos y encaminarnos hacia una autoridad autónoma e independiente para la protección de datos personales. Así mismo se requiere regular esta materia de forma sectorial, especialmente en el ámbito de salud, que incluya el escenario digital.

Aun con riesgos graves para la salud pública, se debe procurar, en la medida de las posibilidades, usar datos anonimizados, encriptados, o recolectar información que al ser cruzada no permita la identificación de las personas.

La garantía del derecho a la protección de datos también depende del adecuado diseño de las herramientas tecnológicas y nuevos modelos de gobernanza de la información, lo que significa que en su desarrollo deben participar no solo expertos en sistemas de información, sino también científicos de datos, especialistas en inteligencia artificial, en bioética, bioderecho, y en derechos humanos.

Esta pandemia ha hecho evidente los riesgos asociados con el analfabetismo digital, pero también el desconocer los riesgos asociados con estas nuevas tecnologías y el haz de facultades con las que contamos los ciudadanos para garantizar el derecho a la protección de nuestros datos personales.

Referencias bibliográficas

- Asociación Médica Mundial (2017). *Declaración sobre epidemias y pandemias.* Adoptada en la 68ª Asamblea General de la AMM, Chicago, Estados Unidos, octubre 2017. https://www.wma.net/es/policies-post/declaracion-sobre-las-epidemias-y-pandemias/.
- Blofield, M., Hoffmann, B., & Llanos, M. (2020). Assessing the Political and Social Impact of the COVID-19 Crisis in Latin America. *GIGA Focus Lateinamerika, 3.*
- Circular Externa 001 de 2020. "Suministro de información al Departamento Nacional de Planeación (DNP) y demás entidades estatales que las requieran para atender, prevenir, tratar o controlar la propagación del COVID-19 (coronavirus) y mitigar sus efectos". Superintendencia de Industria y Comercio, Bogotá, 23 de marzo de 2020. https://www.sic.gov.co/sites/default/files/normatividad/032020/Circular%20001.pdf.pdf.
- Circular Externa 002 de 2020 "No uso de "huelleros físicos o electrónicos" de uso masivo para recolectar información biométrica (datos sensibles) con miras a prevenir el contagio del COVID-19 a través de contacto indirecto". Superintendencia de Industria y Comercio, Bogotá, 24 de marzo de 2020. https://www.sic.gov.co/sites/default/files/normatividad/032020/CIRCULAR%20002%20DE%202020_NO%20USO%20DE%20HUELLEROS.pdf.
- Circular 0017 de 2020 "Lineamientos mínimos a implementar de promoción y prevención para la preparación, respuesta y atención de casos de enfermedad por COVID-19 (Coronavirus)". Ministerio del Trabajo, Colombia, 24 de febrero de 2020. https://www.mintrabajo.gov.co/documents/20147/0/Circular+0017.pdf/05096a91-e470-e980-2ad9-775e8419d6b1?t=1582647828087.
- Comisión Interamericana de Derechos Humanos (2020). *Resolución 01 de 2020, Pandemia y Derechos Humanos en las Américas.* Organización de los Estados Americanos. https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf.
- Consejo de Europa (1997). Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina del Consejo de Europa. https://www.boe.es/buscar/doc.php?id=BOE-A-1999-20638.
- Corte Constitucional (6 de octubre de 2012). Sentencia C-748 de 2011(MP Jorge Ignacio Pretelt Chaljub).

- Decreto 1377 de 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012". Ministerio de Industria, Comercio y Turismo. Diario Oficial de la República de Colombia, No. 48.834, Bogotá DC, 27 de junio de 2013.
- Decreto 417 de 2020 "Por el cual se Declara un Estado de Emergencia Económica, Social y Ecológica en todo el territorio nacional". Presidencia de la República de Colombia, Bogotá, Diario Oficial de la República de Colombia, No 51259, 17 de marzo 2020. http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30038962.
- Decreto Legislativo 538 de 2020 "Por el cual se adoptan medidas en el sector salud, para contener y mitigar la pandemia de COVID-19 y garantizar la prestación de los servicios de salud". Presidencia de la República, Ministerio de Salud y Protección Social. Diario Oficial de la República de Colombia, No. 51283, Bogotá, 12 de abril de 2020. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20538%20DEL%2012%20DE%20ABRIL%20DE%202020.pdf.
- Directrices 04 de 2020 "Sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19". Comité Europeo de Protección de Datos Personales, 21 de abril de 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf.
- Espiérrez, M. A. C. (2016). El derecho a ser informado como elemento esencial del derecho a la protección de datos. Una visión crítica de la jurisprudencia del Tribunal Constitucional y de su cambio de doctrina en la STC 39/2016. *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria*, 106, 191-216.
- Esquivel-Guadarrama, J. A. (2020). Pandemia 2020. Algunas consideraciones éticas. *Revista Mexicana de Anestesiología 43,* 2, 168-172.
- International Bioethics Committee (2017). *Report of the IBC on big data and health*. United Nations Educational, Scientific and Cultural Organization. http://unescoblob.blob.core.windows.net/pdf/UploadCKEditor/REPORT%20OF%20THE%20IBC%20ON%20BIG%20DATA%20AND%20HEALTH%20%2015.09.17.pdf.
- Instituto Federal al acceso de información y protección de datos. (2012). *Guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO.* México. http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf.

- Ley Estatutaria No. 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales". Diario Oficial de la República de Colombia, No. 48.587, Bogotá DC, 18 de octubre de 2012.
- Ministerio de Salud y Protección Social. *Medidas frente a la pandemia COVID-19.* Recuperado el 28 de junio de 2020 de https://www.minsalud.gov.co/salud/publica/PET/Paginas/Documentos-Administrativos-covid-19.aspx.
- Ministerio de Tecnologías de la Información y las Comunicaciones (2020). Abecé/ Todo lo que debe saber sobre CoronApp-Colombia y su funcionamiento. https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126572:Abece-Todo-lo-que-debe-saber-sobre-CoronApp-Colombia-y-su-funcionamiento.
- Murillo, J. G. G. (2016). Elementos esenciales en la protección de los derechos "ARCO". *Letras Jurídicas*, *23*(23).
- Observatorio de Bioética y Derecho. (2015). Comercializar los datos sanitarios: anonimizar no es una respuesta para la bioética. *Revista de bioética y derecho* 33,1-2.
- Open Web Application Security Project (OWASP). Introduction to the OWASP Top Ten. Recuperado el 29 de junio de 2020 de https://owasp.org/www-chapter-new-zealand/assets/slides/2020-02-09%20-%20Introduction%20to%20the%20OWASP%20Top%20Ten.pdf.
- Organización Mundial de la Salud (2017). *Pautas de la OMS sobre la ética en la vigilancia de la salud pública*. Organización Panamericana de la Salud. Washington DC: OPS. https://iris.paho.org/bitstream/handle/10665.2/34499/9789275319840-spa.pdf?sequence=6.
- Organización Mundial de la Salud (2020). *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing*. https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1.
- Organización Panamericana de la Salud (2020). *Orientación ética sobre cuestiones planteadas por la pandemia del nuevo coronavirus COVID-19*. https://iris.paho.org/bitstream/handle/10665.2/52142/OPSHSSBIOCOVID-19200008_spa.pdf?sequence=1&isAllowed=y.

- Pierucci, A. & Walter, J.P. (2020). *Joint Statement on the right to data protection in the context of the COVID-19 pandemic*. Council of Europe, Estrasburgo, 30 de marzo de 2020. https://rm.coe.int/covid19-joint-statement/16809e09f4.
- Resolución 2346 de 2007 "Por la cual se regula la práctica de evaluaciones médicas ocupacionales y el manejo y contenido de las historias clínicas ocupacionales". Ministerio de la Protección Social, Colombia, 11 de julio de 2006. https://www.minsalud.gov.co/ihc/Lists/Resoluciones/DispForm.aspx?ID=4&ContentTypeId=0x0100F912A783706DBF4AA773245C7D7E11F8.
- Resolución 385 de 2020 "Por la cual se declara la emergencia sanitaria por causa del coronavirus COVID-19 y se adoptan medidas para hacer frente al virus". Ministerio de Salud y Protección de Social, Colombia, 12 de marzo de 2020. https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/resolucion-385-de-2020.pdf.
- Resolución 666 de 2020 "Por medio de la cual se adopta el protocolo general de bioseguridad para mitigar, controlar y realizar el adecuado manejo de la pandemia del Coronavirus COVID-19". Ministerio de Salud y Protección Social, Colombia, 24 de abril de 2020. https://id.presidencia.gov.co/Documents/200424-Resolucion-666-MinSalud.pdf.
- Resolución 12169 de 2020 "Por la cual se dictan medidas para garantizar el debido proceso administrativo y la efectiva prestación del servicio de la Superintendencia de Industria y Comercio, en el marco del Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional". Superintendencia de Industria y Comercio, Colombia, 31 de marzo de 2020. https://www.sic.gov.co/sites/default/files/normatividad/042020/res%2012169.pdf.
- Seoane, J. A. (2002). De la intimidad genética al derecho a la protección de datos genéticos: la protección iusfundamental de los datos genéticos en el derecho español (a propósito de las SSTC 290/2000 y 292/2000, de 30 de noviembre) (Parte I). *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada* 16, 71-106.
- SIC analiza manejo de datos de app's para control de Coronavirus (02 de junio de 2020). Portafolio. https://www.portafolio.co/economia/noticias-coronavirus-sic-analiza-manejo-de-datos-de-app-s-para-control-de-coronavirus-541372.
- Silva, D. S., & Smith, M. J. (2015). Limiting Rights and Freedoms in the Context of Ebola and Other Public Health Emergencies: How the Principle of Reciprocity Can Enrich the Application of the Siracusa Principles. *Health and human rights*, *17*(1), E52–E57.

- Superintendencia de Industria y Comercio. *Datos personales y coronavirus COVID-19: recolección y uso de datos en casos de urgencia médica o sanitaria*. Recuperado el 26 de junio de 2020 de https://www.sic.gov.co/slider/datos-personales-y-coronavirus-covid-19-recolecci%C3%B3n-y-uso-de-datos-en-casos-de-urgencia-m%C3%A9dica-o-sanitaria.
- The state in the time of COVID (28 de marzo 2020). The Economist. https://www.economist.com/leaders/2020/03/26/the-state-in-the-time-of-covid-19.
- UN Commission on Human Rights (1984). The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4. Recuperado el 30 de junio de 2020 de https://www.refworld.org/docid/4672bc122.html.
- Voo, T. C., Clapham, H., & Tam, C. C. (2020). Ethical implementation of 'immunity passports' during the COVID-19 pandemic. *The Journal of Infectious Diseases*, jiaa352, https://doi.org/10.1093/infdis/jiaa352.

Fecha de recepción: 1 de julio de 2020
Fecha de aceptación: 8 de julio de 2020