Protección de Datos Personales en el Marco de la COVID-19: el Caso de CoronApp en Colombia

Personal Data Protection in the COVID-19 Context: the Colombian CoronApp Case

Submitted: 27 July 2021
Revised: 11 August 2021
Accepted: 2 December 2021

Article submitted to peer blind review

Karen Isabel Cabrera Peña[*]
https://orcid.org/0000-0003-1285-5500

Yamile Andrea Montenegro Jaramillo[**]
https://orcid.org/0000-0003-2509-9863

DOI: https://doi.org/10.26512/lstr.v14i1.39063

Abstract

[Purpose] *Identify the shortcomings that politics present in the processing of CoronApp data, in contrast to the internal regulations that protect the handling of personal data in Colombia*

[Methodology/Approach/Design] *The research is of a qualitative work where, through the file review, are analyzed the normative documents of the protection of personal data in Colombia in contrast with the data processing policies of the CoronApp application.*

[Findings] *This work concluded that it is necessary to know the handling that is giving to the data so far, to verify if it is feasible to continue using it and, if so, restructure those policies so that it complies with the legal requirements.*

[Practical implications] *This article provides evidence about the shortcomings that the CoronApp application presents about handling personal data and the consequences of their lack of protection. In that sense modification the normative according to the internal regulations is urging, since could cause damages to the holders of those rights. In addition, the article presents some recommendations on how these modifications have to be presents.*

[Originality] *CoronApp application has been recently implemented in Colombia, as a technological solution to collaborate in the management and containment of the COVID-19 virus, is nourished by a series of data that needs to be protected. However, few are the studies that show whether it complies with the legal requirements to protect personal data and which could be the consequences of lack of protection.*

[*] Profesora asistente de la Facultad de Derecho de la Universidad del Norte (Colombia), Abogada de la misma universidad y Doctora en Derecho de la Universidad del Rosario (Colombia). E-mail: cabrerak@uninorte.edu.co.

[**] Profesora asociada en el Programa de Negocios Internacionales de la Universidad El Bosque (Colombia), Máster en Globalización, Comercio Internacional y Mercados Emergentes de la Universidad de Barcelona (España), Doctora en Derecho de la Universidad de Viena (Austria). E-mail: andrea.montenegroj@gmail.com.

***Keywords**: COVID-19. Technology. Personal Data. CoronApp. Colombia.*

Resumen

[Propuesta] Identificar las falencias que presentan las políticas del tratamiento de datos de CoronApp, en contraste con la normativa interna que protege el manejo de datos personales en Colombia.

[Metodología/Enfoque/Diseño] La investigación es de corte cualitativo donde, a través de la revisión de archivo, se analizan los documentos normativos de la protección de datos personales en Colombia y se contrastan con las políticas de tratamiento de datos de la aplicación CoronApp.

[Resultados] Se concluye que es necesario conocer el manejo que se le ha dado hasta ahora a los datos, para verificar si es viable que se continúe con su utilización -respecto a las consecuencias jurídicas de su uso- y, en caso de que así sea, reestructurar dichas políticas para que cumpla con las exigencias legales.

[Implicaciones Prácticas] Este artículo aporta evidencia sobre las falencias que presenta la aplicación CoronApp y las posibles consecuencias de dichas deficiencias respecto al manejo de datos personales. Lo anterior, para instar a que se modifiquen las políticas según la normativa interna, pues es posible que se ocasionen perjuicios a los titulares de estos derechos. Además, se presentan algunas recomendaciones sobre cómo deben hacerse dichas modificaciones.

[Originalidad] La aplicación CoronApp que se ha implementado hace poco en Colombia como una solución tecnológica para colaborar en el manejo y la contención del virus COVID-19, se nutre de una serie de datos que requieren ser protegidos. Pocos son los estudios que dan cuenta de si la aplicación cumple con los requerimientos legales para proteger datos personales y cuáles son las posibles consecuencias jurídicas en su falta de protección.

Palabras Claves: COVID-19. Tecnología. Datos Personales. CoronApp. Colombia.

INTRODUCCIÓN

La emergencia mundial sanitaria por Coronavirus (COVID-19) ha generado la necesidad de establecer medidas restrictivas a los individuos como confinamientos y distanciamiento social. Ante esta situación, la tecnología, a través de inteligencia artificial, blockchain, nanotecnología, aplicaciones móviles, entre otros, se ha constituido en un instrumento que facilita, en particular, información sobre el estado de salud de las personas y la propagación de nuevos contagios, que es utilizada por los Estados para tomar decisiones gubernamentales que permitan contener la enfermedad (YUNIARTE y RATNANINGSIH, 2020, p.7).

Algunos autores señalan que uno de los métodos más empleados para identificar las condiciones del virus, comprenderlo y establecer planes de contingencia es la recolección de datos (GALINDO *et al.*, 2020, p.6), por medio

de aplicaciones de teléfonos móviles (OLIVER *et al.*, 2020 p. 8) pues su tecnología permite obtener información geográfica del usuario, recopilar datos como el estado de salud del mismo y crear cartografía geográfica para tomar medidas sanitarias según condiciones de salubridad en lugares específicos (LYSEEN *et al*., 2014, p.115; ALEUY, PITESKY y GALLARDO, 2018, p.228).

A pesar de las ventajas, existe preocupación sobre qué pasa con la información recopilada ya que, además de ser privada, puede no ser correcta o verídica, lo que puede ocasionar perjuicios a titulares y terceros. En el caso de aplicaciones como Self-quarantine safety protection en Corea del Sur, PeduliLindungi, utilizada en Indonesia o el proyecto Maguen en Israel (CASCON, 2020, p. 4), si bien tenían como objetivo obtener mayor conocimiento para luchar contra el virus, presentaron falencias en la protección a datos privados debido a que no contaban con una política de protección de datos clara, en algunos casos transmitían datos sin autorización de los usuarios o con información poco precisa (SUNYAEV *et al.*, 2015, p. 30, HUCKVALE *et al.*, 2015, p.6) y presentaron limitaciones en relación con el periodo de conservación de los datos (YUNIARTI y RATNANINGSIH, 2020, p.8).

Teniendo en cuenta que los Estados son quienes deben asegurar que el uso de la tecnología garantice la privacidad y la protección de los datos suministrados por los individuos (IENCA y VAYENA, 2020, p.463) y son latentes las vulneraciones que pueden presentarse al derecho a la protección de datos personales en estos escenarios, se procederá a analizar la aplicación CoronaApp, que es utilizada en Colombia para rastrear información sobre la situación y evolución del virus COVID-19 en el país, con el fin de primero, verificar si se protege, o no, el derecho en mención según la normativa interna; segundo, determinar las consecuencias en la falta de protección de estos datos y tercero, presentan algunas recomendaciones sobre cómo deben hacerse dichas modificaciones.

TECNOLOGÍAS USADAS PARA RASTREO DE CONTACTOS EN EL CONTEXTO DE LA COVID-19. EL USO DE APLICACIONES MÓVILES Y CORONAPP EN COLOMBIA

Las aplicaciones móviles que usan tecnología para permitir el rastreo de contactos y así obtener información, en el caso de las empleadas para recopilar datos de la COVID-19, tienen como objetivo determinar geográficamente dónde hay individuos que son portadores del virus a través de Bluetooth, GPS o Wifi (BID, 2020, p.7). En el caso del uso de Bluetooth, este permite entre sus funciones que usuarios con móvil y que se han registrado en estas plataformas, sepan si otra persona cercana está infectada.

Sobre su interoperabilidad, las aplicaciones pueden ser de naturaleza centralizada o descentralizada. En la primera, la entidad de gobierno que gestiona la aplicación tiene la posibilidad de acceder a los datos e incluso compartirlos, incluyendo aquellos provenientes de los otros móviles con los que haya interactuado (ÇELIK Y ÇELIK, 2021, p. 5); en la segunda, el usuario no debe suministrar ningún dato, y la entidad de gobierno no tiene acceso a las interacciones generadas y, en caso de una notificación de un usuario con un reporte positivo, le será asignado un código que deberá registrar en el teléfono y este, a su vez, será compartido con una lista de códigos para verificar con quién estuvo en contacto (BID, 2020, p.11).

De acuerdo con lo anterior, el sistema o enfoque descentralizado es aquel que respeta en mayor medida los derechos de privacidad, ya que el usuario no debe compartir ningún dato (BID, 2020, p.11). Sin embargo, la tendencia en los países, como es el caso de Colombia, Corea del Sur y España, ha sido el uso de aplicaciones de naturaleza centralizada pues los métodos cartográficos, temporales y geo-estadísticos requieren de información detallada para hacer una mejor identificación, rastreo y vigilancia de la propagación de las enfermedades, sobre todo cuando estas son infeccionas (CASCÓN, 2020, p. 3).

En el caso de aplicaciones en el marco de la COVID-19, Self-quarantine safety protection de Corea del Sur no es de uso obligatorio, al menos que sean personas que ingresen al país desde el extranjero (SANTIRSO, 2020). Opera con geolocalización y registrando los datos personales de los usuarios sobre su estado de salud, a partir de unas respuestas a preguntas (App de autoevaluación), lo que permite un diagnóstico masivo de la enfermedad a partir de la información que únicamente es recopilada a través de esta plataforma (CASCÓN, 2020, p. 7).

En el caso de España, con la aplicación Asistencia COVID-19, además de tener las características de Self-quarantine safety protection de la que fue copiada, permite gestionar citas cuando se auto reporta síntomas, lo que implica que la información no solo quede con la entidad que hace el rastreo, sino que se comparta con las autoridades de salud competentes para que analicen y gestionen información que permita derivar al paciente a los servicios que requiera (CASCON, 2020 p. 5).

Otros países que evidencian la viabilidad en la utilización de estas herramientas para el estudio, rastreo y vigilancia de la COVID-19 son Singapur con la aplicación TraceTogether que también utiliza el sistema de rastreo por medio del registro cifrado del contacto para tener mayor control en caso de que alguno de los usuarios sea diagnosticado con el virus o tenga síntomas (CHO, IPPOLITO y YU, 2020, p. 10), e Israel que también utiliza la geolocalización con la aplicación Maguen que a través de GPS trastea a los usuarios (CASCÓN, 2020, p. 5)

Objetivo y Funcionamiento de CoronaApp

En Colombia la aplicación creada por el gobierno en marzo del año 2020 y aun en uso, denominada CoronApp, tiene como objetivo identificar cuáles son las zonas más afectadas y personas con síntomas o diagnosticadas con COVID-19, recopilando datos que van al Centro de Operaciones de Emergencias del Instituto Nacional de Salud, que es la entidad encargada de coordina el sistema de vigilancia en salud pública en el país (INS, *s.f)*. Adicionalmente, ofrece información actualizada sobre la evolución del virus, así como recomendaciones para prevenir el contagio y ubicación de Centros de Salud en donde pueden ser atendidos (CORONAPP - COLOMBIA, *s.f*).

Sobre la iniciativa para crear la aplicación, el Instituto Nacional de Salud (INS) encargó a la Agencia Nacional Digital (AND)[1] para que en compañía de las entidades gubernamentales Ministerio de Tecnologías de la Información y las Comunicaciones, y la Consejería de Transformación digital de la Presidencia de la República la desarrollen. En este sentido, el INS requiere información sobre el estado de salud de la población, pero sobre todo demanda el reporte de personas con síntomas del virus para poder hacer un seguimiento de este (AND, *s.f).*

Teniendo en cuenta lo anterior, las entidades encargadas crean la aplicación con el método de autoevaluación para recopilación de datos y con sistemas de geolocalización a través de Bluetooth y GPS, pues estas dos características permiten establecer el momento de inicio de síntomas de quien decide registrar su información, saber dónde se encuentra concentrado el virus y las potenciales relaciones con otras personas (AND, La historia detrás de CORONAPP, *s.f).*

Ahora bien, la implementación del sistema de autoevaluación por parte del usuario y la activación del Bluetooth para fines de geolocalización implican el manejo de datos personales de quien accede a la aplicación, por lo que fue necesario que se estipularan unos términos y condiciones de uso, así como unas políticas de tratamiento de datos, para cumplir con las reglas mínimas que requiere la ley que debían ser acordes con los protocolos de seguridad tecnológicos de la misma (AND, La historia detrás de CORONAPP, *s.f).*

De esta forma, cuando la aplicación es instalada y el usuario se registra, acepta unos términos y condiciones que se constituyen en un acuerdo de colaboración entre el ciudadano y el Instituto Nacional de Salud, que es quien primariamente recibe los datos. Así, estos términos notifican que se intercambian señales con teléfonos cercanos que también tiene la aplicación, a través de Bluetooth, en donde se hace una identificación anónima encriptada que cambia constantemente para garantizar la privacidad (CORONAPP - COLOMBIA, *s.f*).

[1] Asociación civil, descentralizada que articula servicios ciudadanos digitales (AND, s.f)

Algunos de los datos recopilados por la aplicación son el reporte de estado de salud, síntomas del usuario y de sus familiares, como también su ubicación geográfica en caso de que se encuentre activado el GPS o, en su efecto, el Bluetooth del móvil. Con relación al tratamiento de los datos, el Instituto Nacional de Salud se compromete a la utilización de la herramienta Sistema Nacional de Vigilancia en Salud Pública (SIGIVILA) que es la base de datos del organismo para que estos sean anónimos y no sea posible su vinculación a una persona en particular. Cabe mencionar que SIVIGILA realiza cruce de datos entre INS y las secretarias de salud de las entidades territoriales del país, con el fin de identificar los posibles casos riesgosos, aplicar la prueba de diagnóstico del virus y hacer seguimiento del paciente en caso de que resulte positivo (CUBILLOS y RESTREPO, 2020)

De todos modos, los términos y condiciones manifiestan que los datos serán utilizados única y exclusivamente con fines de vigilancia de la salud pública y se tratarán de acuerdo con la Ley 1581 de 2012 y sus decretos reglamentarios que, como se estudiará a continuación, son el marco regulatorio en la protección de datos personales en Colombia.

REGULACIÓN LEGAL EN LA PROTECCIÓN DE DATOS PERSONALES. DE LO GENERAL HACIA SU NORMATIVA EN COLOMBIA

De manera general, los primeros antecedentes internacionales sobre la protección de datos emanaron del derecho a la privacidad. Por ejemplo, en la Declaración Universal de Derechos Humanos de 1948 y en el Pacto de Derechos Civiles y Políticos de 1966 se habla de la prohibición de injurias arbitrarías o ilegales sobre la vida privada de las personas y aunque no hace referencia a la protección de datos como un derecho autónomo, se infiere que es necesaria la protección de la información que hace parte de la esfera íntima de las personas (LÓPEZ, 2014 p. 107).

De forma más concreta, la Observación General No. 16 del Comité de Derechos Humanos de las Naciones Unidas de 1988 indica que las autoridades competentes, en aras de proteger la vida privada, deben pedir únicamente la información que resulte indispensable para el interés de la sociedad y, de igual forma, establece que la recopilación y el registro de información personal en computadores, bases de datos y otros dispositivos, de cualquier tipo de entidad, debe estar reglamentada por la ley (ASAMBLEA GENERAL DE NACIONES UNIDAS, 1948).

Más adelante, en la Resolución No. 45/95 de 1990, Adoptado por la Asamblea General de la Organización de Naciones Unidas (ONU), respecto a la protección de datos personales en entornos digitales, se indican los principios que deben

implementar los Estados para su protección en modalidades de ficheros computarizados o de equipos informáticos, como por ejemplo el principio de licitud y lealtad, el principio de finalidad y el principio de acceso.

En esta misma línea, son las Directrices adoptadas por la Organización para la Cooperación y el Desarrollo Económico[2] (OCDE) las que, entre otras cosas, definen como dato personal a cualquier información relacionada con un individuo identificado (OCDE, 1980). Respecto a la protección de estos, establece que las directrices son aplicables para los datos personales de cualquier sector -público o privado- y que su protección debe propender la privacidad y las libertades individuales.

Sobre las directrices más relevantes, está que la recolección de datos personales debe hacerse por medios legales y con consentimiento del sujeto (principio de limitación de recogida), que los datos personales recolectados deben ser relevantes para un propósito que no puede excederse de este (principio de especificación del propósito y principio de limitación del uso) y que deben ser exactos, completos y actuales (principio de calidad de los datos). De igual forma, que los datos personales deben ser protegidos contra riesgos (principio de seguridad) (OCDE, 1998).

Por su parte, la Unión Europea ha estipulado un reglamento de protección de datos que expresa que deben entenderse como personales aquellos que identifican físicamente a una persona, lo que no incluye los datos clínicos, sin que esto no signifique que sean datos que gozan de reserva (MONTANARI VERGALLO, ZAAMI, MARINELLI, 2021, p. 23). De igual forma, tienen el General Data Protection Regulation (GDPR) que establece que las leyes de tratamiento de datos personales en los países que conforman la comunidad deben basarse en principios como la rectificación, supresión, restricción de la información, entre otros (CORDEIRO, 2021, p. 63); además, que el procesamiento de datos debe hacerse según el propósito de la recopilación y tratamiento de los mismos durante un tiempo determinado (TORRES, 2019, p. 2)

En el caso de Latinoamérica, Chile cuenta con la Ley No. 19.628 de 1999 que es la que regula la protección de la vida privada o la protección de datos personales. Entre los asuntos regulados está la lista de derechos del titular de los datos en el tratamiento de estos, como son el derecho a la modificación cuando la información está errada (TÍTULO II); ahonda en la autorización del titular de los datos en donde da su consentimiento y este debe ser por escrito sin importar si son recogidos de manera tradicional o digital (TÍTULO III); y también desarrolla lo concerniente a la calidad y licitud de los datos donde anuncia que debe haber un

[2] Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980) y Declaración ministerial sobre la protección de la privacidad de las redes globales (1998).

uso de los mismos respecto a la finalidad para la que fueron recogidos (TÍTULO V).

Igualmente, Argentina tiene la Ley 25.326 de 2000 que regula protección de datos personales. Además de consignar los principios rectores de manejo de datos y consignar los derechos de los titulares de los mismos (CAPÍTULO 1 y 2), crea la Dirección Nacional de Protección de Datos Personales, que es actualmente la entidad encargada de registrar, gestionar y controlar las bases de datos que circulan en el país (INFOLEG, *s.f)*.

Adicionalmente, es importante mencionar que desde la sociedad civil surgen movimientos que buscan manifestarse frente al tratamiento de datos en el ámbito digital. La Carta Internacional de datos abiertos pretende -principalmente- que los derechos de los ciudadanos estén protegidos, promoviendo la transparencia y la responsabilidad de los gobiernos en temas que son de interés colectivo como el cambio climático o la salud pública (MEDIUM, 2020). De igual forma, a nivel latinoamericano la Red Iberoamericana de Protección de Datos (RIPD o Red) ha presentado los "Estándares de Protección de Datos de los Estados Iberoamericanos", que se constituyen en un conjunto de lineamientos normativos en el área de la protección de datos personales con el ánimo de orientar a los países en su regulación y establecer un marco común que sirva como referente garantizando la protección a este derecho en la región (PORCELLI, 2019, p. 472).

Desarrollo Normativo y Jurisprudencial en Colombia

En el caso de Colombia, a grandes rasgos, la protección de los datos personales, conocido constitucionalmente como Derecho de Habeas Data, se encuentra consignado en el artículo 15 de la Constitución Política de 1991 que señala que todos los individuos tienen derecho a conocer, actualizar y rectificar las informaciones que se encuentren en bases de datos de entidades de cualquier tipo. Además, indica que en la recolección, tratamiento y circulación de datos se debe respetar la libertad y demás derechos; y que todas las formas de comunicación privadas son inviolables, sin embargo, pueden ser interceptadas o registradas mediante orden judicial, según establezca la ley.

Como se observa, el artículo desarrolla de manera muy escueta el derecho de Habeas Data, pero es entonces la Ley Estatutaria 1266 de 2008, desplegada por los Decretos 1727 de 2009 y el Decreto 2952 de 2010, la que dispone las reglas sobre el tema y regula el manejo de la información personal contenida en bases de datos, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

De manera general, uno de los artículos relevantes de la ley es el tres que indica que debe entenderse como dato personal a cualquier información,

vinculada, o no, a una o varias personas determinadas, o que pueda asociarse a una persona natural. De igual forma, clasifica los datos personales en públicos, cuando se encuentran contenidos en documentos públicos, como los relativos al estado civil de las personas que no requieren autorización del titular para conocerse; semiprivados, cuando no tiene naturaleza íntima, reservada ni pública, pero su conocimiento o divulgación puede interesar, no solo al titular, sino a otras entidades o personas, como es el caso de los datos financieros que sí requieren autorización del titular con algunas excepciones y, por último, privados cuando se refiere a la esfera íntima o reservada y solo es relevante para el titular y requiere también autorización de este.

Dado que la Ley Estatutaria 1266 de 2008 y sus decretos reglamentarios no fueron suficientes para regular el derecho de Habeas Data por orientarse a la protección de datos comerciales y financieros (ROJAS, 2014, p. 123), se expide la Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto Reglamentario 1377 de 2013, sobre la regulación del derecho fundamental de Habeas Data sobre información registrada en cualquier base de datos que realice operación de recolección.

De las novedades a mencionar, la ley en sus definiciones (ARTÍCULO 3) distingue entre el encargado del tratamiento, que es cualquier persona, que por sí sola o en asocio con otros, realice tratamiento de datos personales, respecto del responsable del tratamiento, que es aquella que decide sobre la base de datos y/o el tratamiento de datos.

En el artículo 5, sobre categoría especiales de datos, se incorpora el dato sensible que se entiende como aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, como lo referente al origen racial o étnico, la orientación política, las convicciones religiosas, la orientación sexual, etc. Por regla general, se prohíbe el tratamiento de datos sensibles, salvo las excepciones taxativamente expuestas en el artículo 6.

Para finalizar con las generalidades, respecto al consentimiento, se amplía su forma de realizarse y este puede ser ahora tácito (DECRETO REGLAMENTARIO PARCIAL 1377 DE 2013). Además, obliga a las empresas que almacenan datos personales a solicitar autorización a los ciudadanos, por cualquier canal, para recogerlos y utilizarlos y, en caso de no atenderse este precepto o realizar acciones como vender base de datos o se le niegue al ciudadano su derecho a actualizar la información, se impondrán sanciones (ARTÍCULOS 14 y 15).

Respecto a la jurisprudencia, la Corte Constitucional, máximo tribunal que conoce sobre casos de protección a derechos humanos en Colombia (CORTE CONSTITUCIONAL, *s.f*), ha manifestado en Sentencia C-1147 de 2001 que los derechos de las personas sobre sus datos personales que están en plataformas

virtuales, como lo son las aplicaciones, no pueden considerarse vagos, ni abstractos. En otras palabras, la protección al Habeas Data -como derecho fundamental- debe ser tratada de manera concreta con los parámetros y límites establecidos para los casos que ocurren sin importar la plataforma o medio donde se recopilen, almacenen y analicen (SENTENCIA T- 552 de 1997 y SENTENCIA T- 729 de 2002).

Particularmente, la Sentencia T-787 de 2004 y la Sentencia C-1011 de 2008, establecen la aplicación de principios de finalidad, necesidad y utilidad, relacionados principalmente con la recolección, el procesamiento y divulgación de la información personal en diferentes entornos y a través de distintas modalidades, como la virtual. De acuerdo con el principio de finalidad, las mencionadas actividades deben responder a un fin constitucionalmente legítimo, definido en la ley de forma clara, suficiente y previa. El principio de necesidad hace alusión a que la información personal recolectada debe ser aquella estrictamente necesaria y el principio de utilidad refiere a que la administración de la información personal debe cumplir una función determinada.

De igual forma, en sentencias como T-260 de 2012, la Corte Constitucional ha manifestado que la vulneración del Habeas Data puede configurarse en plataformas de datos en donde la información es disponible sin tener en cuenta su naturaleza, lo que se considera un riesgo más elevado que cuando los datos son recopilados por medios convencionales (SENTENCIA T-634 de 2013). Particularmente, el usuario en plataformas virtuales, como redes sociales o aplicaciones, corre riesgo cuando sus datos personales pueden ser utilizados por terceros sin autorización o para fines distintos a los autorizados, lo que puede traer como consecuencia que datos sensibles sean divulgados o se utilicen para modalidades de fraude electrónico.

Sobre las consecuencias de la vulneración al derecho de Habeas Data, la Superintendencia de industria y Comercio (SIC)[3], través de su Delegación para la protección de datos personales, ha emitido varias resoluciones requiriendo a plataformas digitales como Zoom, Google y TikTok, que recolectan y almacenan datos personales a través de sus plataformas, a que implementen medidas necesarias para garantizar que cuentan con la autorización adecuada del usuario para gestionar los mismos.

En el caso de Zoom Video Communications, Inc, establece la obligación de esta a someterse a las disposiciones de la Ley 1581 de 2012, respecto a la responsabilidad frente al tratamiento de datos personales de individuos residentes

[3] Autoridad nacional de protección de la competencia, los datos personales y la metrología legal, protege los derechos de los consumidores y administra el Sistema Nacional de Propiedad Industrial, a través del ejercicio de funciones administrativas y jurisdiccionales (SIC, *s.f*).

en Colombia e insta a implementar medidas de seguridad que eviten la afectación de los derechos humanos y fundamentales de los titulares de los datos (RESOLUCIÓN 74519 DE 2020), como disrupciones en las reuniones, hurto de credenciales, transferencia de información a terceros sin autorización y mal manejo de la información.

En la misma dirección, la Resolución 62132 de 2020, ordena a Tik Tok, en su calidad de responsable del tratamiento de datos que se recolectan a través de la aplicación, a implementar mecanismos adecuados para la obtención de autorización o consentimiento de los representantes legales de menores. Igualmente, en relación con Google LLc, la SIC manifiesta la obligación de demostrar que cuenta con la autorización previa, expresa e informada de los representantes legales de todos los menores de edad que hacen uso de la plataforma y de las medidas de seguridad idóneas para salvaguardar los datos (RESOLUCIÓN 14010 de 2021), esto con el fin, entre otras cosas, de evitar casos de intimidación y/o violencia sexual contra estos.

En relación con la gestión de los datos personales y el derecho a que sean eliminados cuando se deje de utilizar la plataforma digital, mediante Resolución 74828 del 17 de diciembre de 2019, la SIC se pronunció requiriendo a la aplicación de servicios tecnológicos -RAPPI- a suprimir los datos personales de manera oportuna, sin que el ciudadano tenga que solicitarlo. Adicionalmente, considera imprescindible que el responsable de la recolección de los datos establezca con certeza la identidad del titular del dato, con el fin de evitar que suplantadores de identidad autoricen el tratamiento de los datos.

Después de esta información básica sobre la regulación de los datos personales, a continuación, se intentará determinar, teniendo en cuenta las dos leyes marco y decretos reglamentarios sobre Habeas Data los requerimientos mínimos de recolección, almacenamiento y tratamiento de datos.

Requerimientos mínimos legales para la recolección, almacenamiento y tratamiento de datos personales

Para facilitar el estudio de los requerimientos legales para el tratamiento de datos personales, debido a la robustez y cantidad de normativa sobre el tema, se han clasificado las leyes y decretos en principios orientadores que deben tenerse en cuenta en la interpretación, desarrollo y aplicación de la normativa sobre el tema. A partir de ellos, por un lado, se determina las garantías de los titulares de los datos personales para su protección; y por el otro, las obligaciones de los encargados que son quienes almacenan y administran la información -operadores según la Ley 158 - y de los responsables de la información que son las que deciden sobre la misma, que según la Ley 1581 se conocen como “fuente”.

Veracidad o Exactitud

Principio	Literal a, artículo 4 Ley 1266 de 2008 Literal d, artículo 4 Ley 1581 de 2012	La información contenida debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
Garantías titulares	Artículo 15, Constitución Nacional Num 2.2, artículo 6 Ley 1266 de 2008 Literal a, artículo 8 Ley 1581 de 2012 Artículo 22 del Decreto 1377 de 2013	Derecho a que los datos sean verdaderos y se actualicen y rectifiquen, según corresponda y supriman cuando esté expresamente prohibido o cuando haya recolección sin la autorización del titular. La información no puede ser parcialmente falsa, inexacta, incompleta, fraccionada o que induzca en error.
Finalidad		
Principio	Literal b, artículo 4, Ley 1266 de 2008 Literal b, artículo 4 de la Ley 1581 de 2012	La administración de los datos personales debe obedecer a una finalidad legitimada por la Constitución y por ley. La recolección de datos se limitada a los fines que sean pertinentes y adecuados para la cual son recolectados.
Garantías titulares	Literal c, artículo 8, Ley 1581 de 2012	Debe ser informado de manera clara y expresa, previa solicitud, sobre el uso de sus datos personales.
Acceso y Circulación Restringida		
Principio	Literal c, artículo 4, Ley 1266 de 2008 Literal f, artículo 4, Ley 1581 de 2012	La administración solo podrá ser realizada por las personas autorizadas por el titular o por las previstas en la ley. Los datos personales, salvo que sean de público conocimiento, no son accesibles por medio de internet o cualquier otro medio de comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o usuarios autorizados por la ley.
Garantías titulares	Artículo 11, Ley 1581 de 2012 Artículo 21, Decreto 1377 de 2013	Puede solicitar, por cualquier medio, su información personal almacenada. La información debe ser de fácil lectura, sin barreras técnicas que impidan su acceso y corresponder a aquella que se encuentre contenida en la base de datos.
Temporalidad de la Información		
Principio	Literal d, artículo 4, Ley 1266 de 2008	La información personal de un titular no puede ser suministrada a usuarios o terceras personas cuando deje de servir para la finalidad con la que fue creado el banco de datos.
Garantías titulares	Artículo 9, Decreto 1377 de 2013	Derecho frente al responsable y/o el encargado del tratamiento, siempre y cuando la supresión de la información no sea procedente por deber legal o contractual. Puede presentar solicitud y/o reclamo ante la SIC para la supresión de los datos personales cuando vencido el término legal el responsable o el encargado de tratamiento no hubiere eliminado los datos.

Seguridad		
Principio	Literal f, artículo 4, Ley 1266 de 2008 Literal g, artículo 4, Ley 1581 de 2012	Adopción de medidas técnicas, humanas y administrativas (ante la SIC) necesarias para garantizar la seguridad en la información contenida en los registros de los bancos de datos y en las consultas realizadas por los usuarios para proteger la información contra riesgos naturales y riesgos humanos.
Garantías titulares	Literales c y d, artículo 8, Ley 1581 de 2012	Derecho a ser informados, previa solicitud, sobre el uso a sus datos personales, los responsables y los encargados del tratamiento. Se encuentran facultados para exigir el respeto a las condiciones de seguridad y privacidad de la información; así como para presentar ante la SIC queja por dicha infracción, para que inicie las investigaciones pertinentes.
Libertad		
Principio	Literal c, artículo 4, Ley 1581 de 2012	La manipulación de la información solo puede realizarse con el consentimiento previo, expreso e informado del titular. Los datos personales no pueden ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que supla dicho consentimiento.
Garantías titulares	Literales b y e, artículo 8, Ley 1581 de 2012 Artículo 9, Decreto 1377 de 2013	Libertad de decidir quién manipula sus datos personales de carácter semiprivado, privado y sensible. Potestad para revocar la autorización dada a los responsables o a los encargados del tratamiento en cualquier momento mediante un reclamo. Derecho de solicitar prueba de la autorización otorgada al responsable del tratamiento, salvo cuando expresamente se exceptúa como requisito para el tratamiento.
Confidencialidad		
Principio	Literal g, artículo 4, Ley 1266 de 2008 Literal h, artículo 1581 de 2012	Se debe garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento.
Legalidad		
Principio	Artículo 18, Decreto 1377 de 2013	Debe haber uso de procedimientos lícitos para recolectar, acceder y actualizar la información personal.

Table 1 – Sobre Requerimientos Legales para el Tratamiento de Datos Personales según Normatividad.

ANÁLISIS DE LAS POLÍTICAS DE TRATAMIENTO DE INFORMACIÓN (PTI) RELACIONADA CON CORONAAPP

Para llevar a cabo la protección del derecho de Habeas Data, el Literal k del artículo 17 de la Ley 1581 de 2012 y el literal f del artículo 18 de la Ley 1581 de 2012, establecen como deber de los responsables y encargados de los tratamientos

de datos la adopción de políticas internas para el tratamiento de los mismos, bien sea en medio físico o electrónico.

Siendo así, se procede a analizar las falencias de las Políticas de Tratamiento de información (PTI) relacionada con CoronaApp de cara a la normativa sobre el tema, teniendo en cuenta que esta opera como responsable y encargado del tratamiento de la información pues obtiene, maneja y almacena la misma, a través del Instituto Nacional de Salud.

Es pertinente mencionar que las PTI fueron expedidas el 8 de mayo de 2020 y hasta el momento, noviembre de 2021, no han sufrido modificaciones. De igual forma, se informa que la aplicación, desde mayo de 2020 hasta la fecha, sigue en funcionamiento y opera bajo los parámetros legales aquí señalados.

Disposición	Comentarios
Veracidad o Exactitud	
Es una aplicación móvil (…) que permite tener acceso a información actualizada y verás (p. 4)	No explica de dónde es extraída la información. Aun cuando tiene datos en la pestaña de "actualidad" como por ejemplo del Estado de los casos en el país, no es claro que dicha información sea obtenida de los datos que los usuarios han ingresado, lo que no permite saber con exactitud para qué sirven los datos registrados. Debido a que la App es voluntaria y los usuarios pueden activar o desactivar funciones de geolocalización o no actualizar los datos de manera periódica, no es posible que se haga un rastreo real y continuo de los datos, lo que trae como consecuencia que la información almacenada no sea totalmente veraz, completa y actualizada.
Finalidad	
La finalidad del tratamiento de datos es realizar vigilancia en salud pública durante las diferentes etapas para abordar la pandemia (p. 14). A través de acciones como monitorear síntomas, estados de alerta, riesgos y vulnerabilidad relacionados con la enfermedad (Num. IV de la finalidad del tratamiento de datos, p. 14)	La disposición no es clara respecto a cómo los datos (tratamiento) permiten la vigilancia de la pandemia. No señala que utiliza la base de datos SIGIVILA y tampoco que hay cruce de datos con las secretarías de salud. No estipula por qué son pertinentes y adecuados los datos recopilados para vigilar la pandemia.

	La aplicación no arroja información sobre cómo se ha desarrollado el virus según los datos compartidos.
La información recolectada es tratada únicamente para enfrentar la crisis de salud pública ocasionada por el SAR-COV-2 (p. 2).	No explica cómo es tratada la información y tampoco cómo sirve esta para enfrentar la crisis.
Acceso y circulación restringida	
En caso de ser necesario circular esa información (datos personales anonimizados) se remitirán los estrictamente necesarios y anonimizados de tal manera que no se pueda identificar el titular (p. 8)	No estipula cuándo se entiende que es necesario circular información personal (que incluye sensible). No indica cómo opera SIGIVILA respecto a la circulación de datos que es compartida con las secretarías de salud.
En algunos casos, se podrá compartir información a las autoridades de salud para el cuidado de los ciudadanos (MinTic, *s.f*).	Aunque la política de tratamiento de datos no lo menciona, en la página del Ministerio de las TIC del Gobierno, indica que la información recolectada (incluyendo la sensible), a través de la aplicación, podrá ser compartida a otras autoridades de salud sin mencionar en qué contexto y con qué finalidad.
Temporalidad de la Información	
La finalidad del tratamiento de datos es realizar vigilancia en salud pública durante las diferentes etapas para abordar la pandemia (p. 14).	No estipula cuáles son las etapas para abordar la pandemia (indeterminada). No es posible determinar cuándo los datos serán necesarios para abordar la pandemia. No determina cómo se realizará la supresión de los datos.
Seguridad	
CoronApp utiliza diferentes medidas técnicas y procedimientos de seguridad de la información, tendientes a garantizar la integridad, disponibilidad y confidencialidad de todos los datos personales suministrados en CoronApp (incluyendo datos sensibles y de menores de edad). Así mismo, garantizar que se evite su adulteración, pérdida, consulta, uso, acceso o divulgación no autorizada o fraudulenta (Punto 8 de los Términos y condiciones, p. 11)	No hace referencia a cuáles son las medidas técnicas ni procedimientos de seguridad para proteger la información.
El INS cuenta con una política de seguridad de la información y datos personales de obligatorio	Hace menciones generales a que cumple con la ley, a través de una

cumplimiento para el tratamiento de los datos recolectados (De las Medidas de seguridad aplicadas al tratamiento de datos personales, p. 24)	política propia, pero no indica las medidas tecnológicas de protección y tampoco dónde se aloja la información.
Todas las medidas de seguridad son objeto de revisión, evaluación y mejora permanente (p. 24) Las medias serán objeto de monitoreo o auditorías, internas o externas con miras a establecer si funcionan correctamente (…) (p. 10).	Dentro de la aplicación no se encuentran informes sobre auditorías, o sobre revisiones, internas o externas, que se hayan realizado para mejorarla.
Libertad	
La finalidad del tratamiento de datos es realizar vigilancia en salud pública durante las diferentes etapas para abordar la pandemia (p. 14). A través de acciones como permitir la consulta por parte de las autoridades del estatus de movilidad, a través de un código QR (Num. IX de la finalidad del tratamiento de datos, p. 14)	Aunque el uso de la aplicación es voluntario, resulta obligatorio en los casos en los que se pretenda hacer viajes nacionales, aéreos o terrestres (Botero, 2020), puesto que las entidades de movilidad pueden solicitar un código QR específico que es arrojado por la app cuando se ingresan datos como duración del mismo y datos del vuelo, lo que restringe la libertad del usuario a utilizar, o no, la App y la libertad de escoger los datos que desea compartir.
Legalidad	
El INS adoptará las estrategias, procedimientos y herramientas útiles para demostrar ante la SIC que ha implementado medidas apropiadas y efectivas para cumplir con sus obligaciones legales con lo relacionado al tratamiento de datos personales.	Dentro de la aplicación no hay evidencias sobre la implementación efectiva de medidas apropiadas para la protección de la información personal almacenada según los requerimientos legales.

Table 2 – Análisis de Políticas de Tratamiento de Datos de CoronApp según Normativa para el Tratamiento de Datos Personales.

Del anterior análisis y sistematización de las políticas de tratamiento de datos, según la normativa de Habeas Data, se pueden determinar dos grupos de falencias:

- **Por Desconocimiento de la Tecnología:** Sobre este punto, si se observa la redacción de las políticas sobre finalidad, se evidencia que no hay claridad sobre cómo el uso de esta tecnología, pero sobre todo la recolección de estos datos, se convierten en una estrategia para combatir la crisis que ha traído el virus.

De igual forma, al revisar las políticas que computan a los principios de veracidad, en donde la información debe estar actualizada, se desconoce que la geolocalización por Bluetooth o GPS solo arrojará datos continuos y actualizados si los usuarios tienen activo todo el tiempo la función; o en el caso del principio

de seguridad, no se estipula las medidas tecnológicas de seguridad y protección implementadas (si es que las hay), cuando son estas herramientas las que mayor funcionalidades al respecto ofrecen.

Asimismo, la falta de claridad sobre el uso de la tecnología y la operabilidad de la aplicación puede deberse a que esta tiene pocas medidas de evaluación de seguridad de los datos, lo que genera desinformación e inseguridad entre los usuarios, pero sobre todo atención deficiente (CORDEIRO, 2021, p. 21).

Como solución al anterior panorama, donde no hay claridad sobre la responsabilidad de las instituciones sanitarias frente a las posibles falencias de la aplicación, países como Eslovenia han incrementado el estándar normativo con la creación de la Ley de protección de bases de datos en salud para que el instituto de salud pública a cargo no necesite el consentimiento informado del usuario para el procesamiento de datos, pero se restrinja más el acceso a la información, por ejemplo que se limite únicamente al médico tratante (TEPEJ, 2021, p. 3)

De igual forma, en busca de un balance entre la protección de los datos y la accesibilidad a los mismos por medio de desarrollos tecnológicos en el sector salud a través de disposiciones legales, la Unión Europea emitió la Guía 04/2020 sobre el uso de datos de ubicación y herramientas de rastreo de contactos en el marco de la COVID- 19 con el ánimo de salvaguardar los derechos de los ciudadanos (SEVILLA, 2021, p. 5). De esta forma, la guía insta a los países a crear regímenes jurídicos que indiquen el tratamiento detallado que deben tener los datos y la responsabilidad que tiene el encargado frente a los usuarios cuando de servicios médicos se trata (COTINO, 2020, p. 4).

Si bien es cierto que las herramientas en los sistemas de salud pueden llegar a ser instrumentos más fiables que los consentimientos o herramientas manuales, las medidas de rastreo tecnológico, si no se encuentran correctamente diseñadas y reguladas, pueden permitir el acceso a datos personales que pueden usarse y divulgarse de manera ilegal, generándose así un conflicto entre dos derechos fundamentales como la salud pública y la protección de datos (MONTANARI VERGALLO, ZAAMI, MARINELLI, 2021, p. 2451). Este es el caso de Corea del Sur que vulnera el derecho a la privacidad de los ciudadanos al usar como herramienta de seguimiento a los contagiados, además de los sistemas de geolocalización, el rastreo de tarjetas y reconocimiento facial mediante cámaras (CASCÓN, 2020, p. 7)

- **Por Redacción General y Escueta:** La mayoría de las disposiciones estipuladas en las PTI son muy generales y, si bien hacen referencia a las obligaciones normativas, estas no se desarrollan de manera tal que expliquen con claridad cómo CoronApp maneja los datos de los usuarios. Lo anterior, se convierte en una vulneración del derecho de Habeas Data,

> pues según los principios de finalidad, temporalidad, legalidad y seguridad es obligación del encargado y responsable tomar medidas particulares y ajustadas al medio y forma en que se hace la recolección de datos para el manejo legal de los mismos.

Como se evidencia, tampoco se cumplen con las estipulaciones legales de la protección de datos, y es posible que se configuren vulneraciones al derecho de Habeas Data al no determinarse cómo y quién hace el cruce de información en la base de datos SIGIVILA.

En países como India, que implementó un consentimiento general para que los usuarios permitieran el intercambio de datos entre pacientes, proveedores y pagadores en el ecosistema de salud National Digital Health Mision para darle mayor y mejor gestión a la pandemia producida por la COVID-19, se evidencia la misma dificultad que con CoronApp. La redacción de la disposición del consentimiento general, además de generar desconfianza entre los usuarios por ser escueta en su redacción, demostró que es posible que se generen problemas de privacidad de la información pues esta circula entre varias entidades sin saberse con certeza cuál es el tratamiento que le dan a los datos, acentuando la preocupación si se tiene en cuenta que son datos sensibles (SAKSENA, MATTHAN, BHAN *et al.*, 2021, p. 3).

Autores como Churi, Pawar y Moreno (2021), sugieren una mejor articulación entre el trabajo que realizan las entidades de salud y los gestores que hacen el intercambio de datos, con la idea de redactar políticas de tratamiento y condiciones de uso que protejan la privacidad, pero sobre todo que tengan en cuenta las particularidades que tiene el manejo de datos cuando son sobre la salud del usuario por ser sensibles y requerir mayor salvaguarda.

CONCLUSIONES

Desde lo expuesto brevemente en las anteriores líneas, se puede evidenciar que la aplicación CoronApp implementada en Colombia nace, al igual que otros países como España, Israel y Corea del Sur, como una herramienta tecnológica para colaborar en el manejo y control del virus COVID-19 que se ha convertido en una problemática de salud pública que ha afectado a la población mundial.

Particularmente, la aplicación pretende, a partir de sistemas de geolocalización y autoevaluación por preguntas, identificar zonas y personas diagnosticadas con el virus con el fin de recopilar datos que se dirigen a la base de datos SIGIVILA del Centro de Operaciones de Emergencias del Instituto Nacional de Salud, con la finalidad de que dicha información ayude a enfrentar la crisis y se impida su extensión.

Como bien se mencionó, el tratamiento de los datos recogidos por la aplicación toma real relevancia si se tiene en cuenta que la mayoría de esta información, por recaer sobre datos personales, localización del usuario y estado de salud de este, es privada y, en muchos casos, de naturaleza sensible, lo que debe conllevar un grado mayor de protección.

De igual forma, es importante recordar que, dado que el Centro de Operaciones de Emergencias del Instituto Nacional de Salud recolecta, almacena y usa la información personal de los usuarios, implica que sus políticas de uso, y sobre todo aquellas sobre el tratamiento de datos, deban ser lo suficientemente claras, no solamente respecto a la finalidad en la utilización de los datos, sino también sobre las obligaciones que como responsable y encargado tiene el instituto -tal como lo señala la Corte Constitucional-, sobre todo si se tiene en cuenta que dicha información se cruza y comparte con otras entidades como los centros de salud de los diferentes territorios del país.

Ahora bien, sin desconocer que la tecnología y, en particular esta clase de aplicaciones son herramientas loables para generar soluciones en esta clase de crisis y emergencias de salud, a través del estudio que se realizó de las políticas de tratamiento de datos de la aplicación CoronApp, en comparación con la normativa colombiana sobre la protección de bases de datos, que es bastante robusta y se encuentra desarrollada por diferentes herramientas legales, se pueden identificar dos falencias: una, sobre desconocimiento de la tecnología y otra, de la redacción de las políticas, que vulneran el derecho constitucional colombiano de Habeas Data y que, de igual forma, ponen en entredicho la viabilidad y utilidad de la aplicación.

Como se observó en otros países, estas falencias traen consigo falta de confianza en la aplicación, falencias en el servicio, pero sobre todo inseguridad y falta de privacidad en el tratamiento de datos, lo que puede conllevar a fraudes electrónicos, divulgación, transferencia y hurto de información sensible.

Teniendo en cuenta lo anterior, y que no existe hasta el momento denuncia, pronunciamiento oficial o resolución administrativa sobre los asuntos antes mencionados, pero teniendo en cuenta los pronunciamientos de la SIC respecto a casos de tratamiento de datos en aplicaciones, se puede concluir y proponer como plan de mejora tres aspectos básicos. Primero, es imperativo que el Centro de Operaciones de Emergencias del Instituto Nacional de Salud presente un informe sobre cómo funciona la aplicación respecto al manejo y protección de datos y cuáles son las medidas tecnológicas de seguridad que utiliza con la finalidad de conocer cómo se ha venido analizando la información y así determinar, por un lado, si este ha sido acorde a la ley, respecto a aspectos como finalidad y seguridad, y por el otro, dilucidar si realmente CoronApp ofrece soluciones a la crisis de salud pública.

Segundo, las políticas de datos personales deben ser modificadas de tal forma que delimiten asuntos como, por ejemplo, las tareas específicas y determinadas que el Centro de Operaciones de Emergencias del Instituto Nacional de Salud realiza con los datos de los usuarios. En otras palabras, deben eliminarse todas las redacciones genéricas e imprecisas que hacen referencia a la legislación de Habeas Data pues no anuncian y tampoco desarrollan el manejo de los datos, de manera específica, dentro de la aplicación. Todo lo anterior con la finalidad de entender, conocer y asegurar la aplicación de los principios del derecho de Habeas Data.

Otra opción en este punto es que el gobierno decida reglamentar normativa y administrativamente el manejo de datos cuando se trate de aplicaciones que recopilen, gestionen y analicen información de usuarios en asuntos de salud y/o médicos, para evitar posibles infracciones al Derecho de Habeas Data cuando las PTI o condiciones de uso sean escuetas, lo que garantizaría también que los sistemas de seguridad informáticos para la salvaguarda de los datos sean idóneos.

Por último, sería pertinente conocer, para así posteriormente revisar, las medidas tecnológicas que usa la aplicación en asuntos como los que tienen que ver con geolocalización o generación de código QR. Esto con el fin de, primero, verificar que se está limitando el uso de la información a los fines propuestos de la aplicación -aunque estos aún no son claros- y segundo, para corroborar si realmente CoronApp es un insumo que aporta como propuesta al manejo y contención del virus.

REFERENCIAS

Aleuy, O.; Pitesky, M.; Gallardo, R. (2018). Using multinomial and space-time permutation models to understand the epidemiology of infectious bronchitis in California between 2008 and 2012. **Avian diseases,** 62(2), 226-232. https://doi.org/10.1637/11788-122217-Reg.1.

Agencia Nacional Digital (s.f). **¿Quíenes somos?** Recuperado de: https://and.gov.co/nosotros-3/#:~:text=La%20AND%20es%20una%20entidad,de%20la%20ciencia%20y%20las.

Agencia Nacional Digital (s.f). **La historia detrás de CoronApp**. Recuperado de: https://and.gov.co/news/la-historia-detras-de-coronapp/.

BID (2020). **Tecnologías digitales para la notificación de exposición en época de pandemia.** Documento para discusión núm. IDB-DP-00836. Recuperado de: https://publications.iadb.org/publications/spanish/document/Tecnologias-digitales-para-la-notificacion-de-exposicion-en-epoca-de-pandemia.pdf.

Botero C. (2020, septiembre 4). **CoronaApp, voluntariamente obligada para viajar.** El Espectador. Recuperado de: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/coronapp-voluntariamente-obligada-tambien-para-viajar-column/.

Cascón, J. D. (2020). Tecnologías para luchar contra la pandemia COVID-19: geolocalización, rastreo, Big data, SIG, inteligencia artificial y privacidad. **Profesional de la información**, 29(4), e290429. https://doi.org/10.3145/epi.2020.jul.29.

Çelik Ertuğrul D, Çelik Ulusoy D. A (2021). **Knowledge-based self-pre-diagnosis system to predict COVID-19 in smartphone users using personal data and observed symptoms.** Expert Syst. 21:10.1111/exsy.12716. doi: 10.1111/exsy.12716. Epub ahead of print. PMID: 34177034; PMCID: PMC8209830.

Cho, H., Ippolito, D., Yu, Y. (2020). Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. **Revista arXiv:2003.11511**. Recuperado de: http://arxiv.org/abs/2003.11511.

Churi P, Pawar A, Moreno A.J. (2021). A Comprehensive Survey on Data Utility and Privacy: Taking Indian Healthcare System as a Potential Case Study. **Inventions**. 6(3), 45. https://doi.org/10.3390/inventions6030045.

Comité de Derechos Humanos de las Naciones Unidas de (1988). Comentarios generales, Artículo 17. Derecho a la intimidad, U.N. Doc. HRI/GEN/1/Rev.7 at 162, **Observación General Número 16**. Recuperado de: http://www1.umn.edu/humanrts/hrcommittee/Sgencom16.html.

Comité de Derechos Humanos de las Naciones Unidas (1988). **Observación General No. 16.** Recuperado de: https://conf-dts1.unog.ch/1%20SPA/Tradutek/Derechos_hum_Base/CCPR/00_2_obs_grales_Cte%20DerHum%20%5BCCPR%5D.html#GEN16.

Cordeiro J. (2021). Digital Technologies and Data Science as Health Enablers: An Outline of Appealing Promises and Compelling Ethical, Legal, and Social Challenges. Front. Med. 8(8):647897. doi: 10.3389/fmed.2021.647897.

CoronApp Colombia- (s.f.). **Términos y Condiciones.** Recuperado de: http://www.ins.gov.co/Terminos_y_condiciones_CoronApp.pdf

Corte Constitucional (s.f). **La Corte.** Recuperado de: https://www.corteconstitucional.gov.co/lacorte/.

Cotino L. (2020). Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos. **Revista de Internet, Derecho y Política**, 31.

Cubillos, M.C, Restrepo, M.A. (2020) **La CoronAPP-Colombia y su política de tratamiento de datos.** Recuperado de: https://derinformatico.uexternado.edu.co/coroappcolombia/.

Galindo, N.M., Guarino de Moura G., Barbosa L., De Castro, J. Barros A., Moreira L., (2020). COVID-19 and digital technology: mobile applications available for download in smartphones. **Texto Contexto**

Enferm, e20200150https://doi.org/10.1590/1980-265X-TCE-2020-0150.

Huckvale, K., Prieto, J.T., Tilney, M., Benghozi, J.P., Car, J. (2015). Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. **BMC Medicine**, 13, 214. https://doi.org/10.1186/s12916-015-0444-y.

Ienca, M., Vayena E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. **Nature Medice Review**, 26, 463–464.

InfoLEG (sf.). **Dirección Nacional de Protección de Datos Personales**. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/110000-114999/114376/norma.html.

Instituto Nacional de Salud (s.f). **Plataforma estratégica**. Recuperado de: https://www.ins.gov.co/conocenos/plataforma-estrat%C3%A9gica

López, J. (2014). Antecedentes internacionales en materia de privacidad y protección de datos personales. **Journal of Internacional Law**, 5(2), 104-117.

Lyseen, A., Nøhr, N., C.; Sørensen, E.; Gudes, O., Geraghty, E., Shaw N., (2014). A review and framework for categorizing current research and development in healthrelated geographical information systems (GIS) studies. **Yearbook of medical informatics,** 9(1), 110-124. https://doi.org/10.15265/IY-2014-0008.

Medium (2020, Abril 26). **Open principles for data rights.** Recuperado de: https://medium.com/opendatacharter/open-principles-for-data-rights-611d76f475c7.

Mintic (2020, Abril 14). Abecé/ **Todo lo que debe saber sobre CoronApp-Colombia y su funcionamiento**. Recuperado de: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126572:Abece-Todo-lo-que-debe-saber-sobre-CoronApp-Colombia-y-su-funcionamiento.

Montanari G, Zaami S, Marinelli E. (2021). The COVID-19 pandemic and contact tracing technologies, between upholding the right to health and personal data protection. **Eur Rev Med Pharmacol Sci**. 25(5):2449-2456. doi: 10.26355/eurrev_202103_25286. PMID: 33755984.

OCDE (1980). **Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.** Recuperado de: https://www.oecd.org/sti/ieconomy/15590267.pdf.

OCDE (1998). **Declaración ministerial sobre la protección de la privacidad de las redes globales.** Recuperado de: http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_redes.pdf.

Oliver, N., Letouzé, E., Sterly, H.; Delataille, S, De-Nadai, M., Lepri, B. Vink, P. (2020). **Mobile phone data and COVID-19:** Missing an opportunity? Computer and Society. Recuperado de: http://arxiv.org/abs/2003.12347.

Porcelli, A. (2019). La Protección de los Datos Personales en el Entorno Digital. Los Estándares de Protección de Datos en los Países Iberoamericanos. **Quaestio Iuris**, 12(2), 465-497. doi: 10.12957/rqi.2019.40175.

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. **Novusjum**, 8(1), 107-139 https://novumjus.ucatolica.edu.co/article/view/652/670.

Saksena N, Matthan R, Bhan A, Balsari S. (2021). Rebooting consent in the digital age: a governance framework for health data exchange. **BMJ Global Health.** 6:e005057. doi:10.1136/ bmjgh-2021-005057.

Santirso, J. (2020, Marzo 14). Corea del Sur: contra el coronavirus, tecnología. EL PAÍS. Recuperado de: https://elpais.com/tecnologia/2020-03-13/corea-del-sur-contra-el-coronavirus-tecnologia.html.

Sevilla M.A. (2021). Las medidas de contención de la COVID-19 frente al derecho a la protección de datos personales sanitarios de la CDFUE. **Revista de los Estudios de Derecho y Ciencia Política**, 32.

SIC (s.f). **Nuestra entidad.** Recuperado de: https://www.sic.gov.co/nuestra-entidad.

Sunyaev, A., Dehling, T., Taylor, P. L. and Mandl, K. D. (2014). Availability and quality of mobile health app privacy policies. **Journal of the American Medical Informatics Association.** 22(1), 28-33. doi: https://doi.org/10.1136/amiajnl-2013-002605.

Tepej J. (2021). Impact of data protection regulation on Slovenian eHealth. **Journal Glbo Health**, 11, 1-4. doi: 10.7189/jogh.11.03063.

Torres E. (2019). **La Protección de datos personales en Europa y en Colombia, similitudes y diferencias**. Tesis de Especialización de Gerencia de Gerencia Estratégica de Tecnología en Informática, Universidad Santiago de Cali, Facultad de Ingeniería. Dspace. Disponible em: https://repository.usc.edu.co/handle/20.500.12421/2937.

Yuniarti S., Ratnaningsih. E. (2020). Combating COVID-19: Challenge for data protection and privacy. **International Conference on Biospheric Harmony Advanced Research**, 729, 1-9. doi:10.1088/1755-1315/729/1/012115.

Normativa y Otros Documentos Legales

Asamblea General de Naciones Unidas (ONU). Declaración Universal de Derechos Humanos 1948. Recuperado de: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

Asamblea General de Naciones Unidas (ONU). Pacto de Derechos Civiles y Políticos (1966). Recuperado de: https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

Asamblea General de la Organización de Naciones Unidas (ONU). Resolución No. 45/95 de 1990. Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales, 14 de diciembre de

1990. Recuperado de: http://ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf

Constitución Política de Colombia de 1991, Congreso de la República de Colombia, Gaceta Constitucional Nro. 116, (20 de julio de 1991).

Ley Nº 19.628 "*Ley sobre Protección de la vida privada o protección de datos de carácter personal*" Legislador del Estado Chileno, (28 de agosto de 1999)

Ley 25.326 regula la protección de los datos personales en Argentina, (4 de octubre de 2000)

Ley Estatutaria 1266 de 2008, Congreso de la República de Colombia, Diario Oficial 47.219, (31 de diciembre de 2008).

Ley Estatutaria 1581 de 2012, Congreso de la República de Colombia, Diario Oficial 48587, (18 de octubre de 2012). Decreto 1727 de 2009. Presidente de la República de Colombia, Diario Oficial 47350, (15 de mayo de 2009).

Decreto 2952 de 2010. Presidente de la República de Colombia, Diario Oficial 47793, (6 de agosto de 2010).

Decreto Reglamentario 1377 de 2013. Presidente de la República de Colombia, Diario Oficial 48834, (27 de junio de 2013).

Guía Unión Europea 04/2020. Sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, (21 de abril de 2020).

Jurisprudencia de la Corte Constitucional de Colombia

Sentencia T 552/1997 (1997, 30 de octubre) Corte Constitucional (Vladimiro Naranjo, M.P.)
https://www.corteconstitucional.gov.co/relatoria/1997/T-552-97.htm

Sentencia C 1147 / 2001. (2001, 31 de octubre). Corte Constitucional (Manuel José Cepeda, M.P.) https://www.corteconstitucional.gov.co/relatoria/2001/C-1147-01.htm

Sentencia T-729/ 2002 (2002, 5 de septiembre) Corte Constitucional (Eduardo Montealegre, M.P.) https://www.corteconstitucional.gov.co/relatoria/2002/T-729-02.htm

Sentencia T-787/ 2004 (2004, 18 de agosto) Corte Constitucional (Rodrigo Escobar, M.P.) https://www.corteconstitucional.gov.co/relatoria/2004/T-787-04.htm

Sentencia C-1011/ 2008 (2008, 16 de octubre) Corte Constitucional (Jaime Córdoba, M.P.) https://www.corteconstitucional.gov.co/relatoria/2008/c-1011-08.htm

Sentencia T-260/2012 (2012, 29 de marzo) Corte Constitucional (Humberto Sierra, M.P.) https://www.corteconstitucional.gov.co/relatoria/2012/t-260-12.htm

Sentencia T-634/ 2013 (2013, 13 de septiembre) Corte Constitucional (María Victoria Calle, M.P.)

https://www.corteconstitucional.gov.co/RELATORIA/2013/T-634-13.htm

Resoluciones de la Superintendencia de Industria y Comercio de Colombia

Resolución Número 74828 de 2019 (2019, 17 de diciembre) Superintendencia de Industria y Comercio.
https://www.sic.gov.co/sites/default/files/boletin-juridico/Res%2074828%20del%2017XII2019%20Rappi.pdf
Resolución 62132 de 2020 (2020, 5 de octubre) Superintendencia de Industria y Comercio.
https://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/20-106617%20VU%20TIK%20TOK.pdf
Resolución 74519 de 2020 (2020, 23 de noviembre) Superintendencia de Industria y Comercio. https://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/Res%2074519%20DE%202020%20ZOOM(1).pdf
Resolución Número 14010 de 2021. (2021, 16 de marzo) Superintendencia de Industria y Comercio. https://www.sic.gov.co/sites/default/files/normatividad/082021/RE14010-2021.pdf