DOI: 10.13137/2035-6633/31195

Reflexión sobre los límites sociales, políticos y jurídicos a las estrategias de rastreo de contactos epidemiológicos mediante aplicativos móviles. El caso de Medellín (Colombia)

Sebastian Giraldo[*]
Biviana Avila Lasso[**]
Luis Roberto Mercado[***]
Juan Felipe Zapata[**]
Andrés Roncancio Bedoya[*]

Abstract

The authors reflects on contact tracing applications during the Covid-19 pandemic and the risks that these technologies represent for citizens in the absence of policies that regulate and monitor the use of data by institutions.
Keywords: Covid-19, contact-tracing apps, data privacy, security, mobile health

Los autores reflexionan sobre las aplicaciones de rastreo de contactos durante la pandemia de Covid-19 y los riesgos que estas tecnologías representan para los ciudadanos en ausencia de políticas que regulen y hagan seguimiento al uso de los datos por parte de las instituciones.
Palabras claves: Covid-19, aplicaciones de rastreo de contactos, privacidad de datos, seguridad, salud móvil

Gli autori riflettono sulle applicazioni di tracciamento dei contatti durante la pandemia Covid-19 e sui rischi che queste tecnologie rappresentano per i cittadini in assenza di politiche che regolano e monitorano l'uso dei dati da parte delle istituzioni.
Parole chiavi: Covid-19, app di tracciamento dei contatti, privacy dei dati, sicurezza, salute e dispositivi mobili

Introducción

La pandemia de Covid-19 se ha convertido en la primera emergencia de salud pública de impacto global en la actual era digital, pues los anteriores brotes de enfermedades infecciosas se desarrollaron de manera localizada o tuvieron tasas inferiores de infección y muerte a lo que se estimó inicialmente (Fahey, Hino, 2020; Freitas *et al*., 2020).

[*] Institución universitaria de Envigado, Medellín (Colombia); e-mail Sgiraldoh@correo.iue.edu.co; e-mail afroncancio@correo.iue.edu.co.
[**] Corporación universitaria Remington, Medellín (Colombia); e-mail bibiana.avila.3493@miremington.edu.co; e-mail juan.zapata@uniremington.edu.co.
[***] Corporación universitaria Remington, Medellín (Colombia) e-mail luismercado119761@correoitm.edu.co.

Es innegable que las tecnologías de la información y la comunicación (Tic´s) han jugado un rol fundamental en la actual pandemia, muchos sectores económicos se han mantenido activos gracias a las tecnologías del teletrabajo (Lincoln *et al*., 2020; Martin, 2020; Sugestyo Putro, Riyanto, 2020); las redes sociales y plataformas de comunicación digital han desempeñado un papel especial en la conservación de la salud mental de los ciudadanos y en el mantenimiento de sus relaciones sociales durante los periodos de restricción de la movilidad bajo estrategias como el distanciamiento físico, que se estableció globalmente como un mecanismo de contención del virus, su implementación obligó a muchos gobiernos a tomar medidas de cuarentenas y confinamientos (Chan *et al*., 2020; Elmer *et al*., 2020; Marroquín *et al*., 2020; Ni *et al*., 2020), además, se han visto fortalecidas las nuevas estrategias de diagnóstico clínico y se han potencializado los mecanismos de telemedicina, por ejemplo, muchas consultas externas se han convertido a modalidades virtuales, ya sea por teléfono o por video. Estrategias que han contribuido a minimizar la propagación del virus, garantizar el acceso a salud en algunas regiones o para algunas minorías y además han reducido costos en elementos de protección personal (Epp) en el sistema de salud (Leite *et al*., 2020; Martin, 2020; Ortega *et al*., 2020; Pappot *et al*., 2020).

Otro de los impactos positivos de la implementación de las Tic´s es que han favorecido la visualización de datos relacionados con la transmisión del virus en tiempo real, permitiendo a ciudadanos, personal de la salud y tomadores de decisiones la comprensión de este fenómeno de salud-enfermedad, lo cual ha facilitado la rápida comunicación de cuestiones y directrices clave para el manejo de la pandemia en cada País (Verhagen *et al*., 2020).

A medida que la pandemia del Covid-19 se extendió por todo el mundo, se buscaron implementar estrategias de rastreo de contactos epidemiológicos para romper el ciclo de transmisión del Sars-Cov-2, estos consisten en acciones lideradas por el personal de la salud que están encaminadas a la observación y rastreo de forma manual de contactos tras la exposición a una persona infectada con el fin de ayudar a que estas personas reciban atención y tratamiento temprano y así evitar una mayor transmisión de un agente infeccioso, interrumpiendo el ciclo de contagio del virus (Torok, 2005).

Ante este potencial instrumento preventivo, se implementó en varios Países el uso de aplicativos móviles para superar las dificultades que el rastreo manual presentaba, es decir planteó una solución al proceso lento de realizar entrevistas persona a persona y que exigía el despliegue de un gran número de funcionarios en campo para realizar un trabajo investigativo complejo, es por ello que la posibilidad de usar el teléfono móvil para automatizar este proceso de rastreó se presentó como una excelente alternativa (Zastrow, 2020).

Colombia lanzó el 7 de marzo, CoronApp, un aplicativo móvil destinado inicialmente a permitir que el gobierno rastreará los brotes de Covid-19 y almacenamiento centralizado de datos, además de educar al público sobre el virus, la portabilidad de dicho aplicativo se exigió como un pasaporte de movilidad en el País. Su lanzamiento sucedió mucho antes que en la mayoría de Países e incluso antes de

todas las discusiones y avances en políticas de privacidad y almacenamiento de datos descentralizados (Edwards, 2020).

Fue a partir de abril de 2020 que se publicaron los primeros desarrollos tecnológicos destinados a mejorar la capacidad de la comunidad de salud pública para frenar la pandemia de Covid-19 a través de comunicación digital personal respetando políticas internacionales que preservan la privacidad y almacenamiento de datos descentralizado, siendo los proyectos más destacados Trace together (2020) en Singapur, el Grupo de rastreo automatizado de contactos privados (Pact) (European consortium, 2020) dirigido por el Mit y el consorcio europeo de seguimiento de proximidad descentralizado para preservar la privacidad (Dp-3T) (Pact's, 2020).

El 10 de abril, Apple y Google cooperaron con los grupos anteriormente mencionados en una plataforma común de rastreo de contactos (Gapple) que fue lanzada en el mes de mayo, Gapple no es una aplicación sino una plataforma para el desarrollo de aplicativos móviles para el rastreo de contactos el cual ofrece un marco que proporciona una funcionalidad basada en Bluetooth. Estas mejoras garantizan mayor seguridad al realizar la captura de datos de contacto en segundo plano; este protocolo es accesible para las agencias de salud pública que deseen usarlo para sus propias aplicaciones a través de una interfaz de programación de aplicaciones llamada Api de notificación de exposición, que permitirá que estas aplicaciones registren y reciban datos (Gvili, 2020; Michael, Abbas, 2020; Rowe, 2020).

Además, los protocolos implementados en el modelo Gapple son seguros pues no recopila ni rastrea la ubicación del dispositivo; los datos se recopilan en los teléfonos de los usuarios en lugar de en un servidor centralizado, no comparte las identidades de los usuarios con otras personas. Apple, Google o las autoridades sanitarias no tienen acceso directo a los datos y los usuarios pueden continuar usando la aplicación de la autoridad de salud pública sin optar por las notificaciones de exposición de Gapple, y pueden apagar el sistema de notificación si cambian de opinión (Chugh, 2020; Gvili, 2020; Michael, Abbas, 2020).

El 26 de abril de 2020 el gobierno australiano implementó una de las primeras estrategias de aplicativos de rastreo de contactos; en solo 24 horas dicho aplicativo ya contaba con dos millones de descargas. A pesar de esto, su implementación se consideró un fracaso por asuntos relacionados con la seguridad y la privacidad más que por aspectos técnicos al no ajustarse a protocolos Gapple (Chugh, 2020; Rowe, 2020). En los meses posteriores muchos Países implementaron estrategias similares, incrementando las dudas sobre la efectividad de estos aplicativos e intensificando cuestionamientos relacionados con la seguridad y la protección de la privacidad de los usuarios (ServickMay, 2020).

Alemania realizó esfuerzos para la creación de un consorcio europeo construido en torno a un enfoque centralizado llamado Seguimiento de proximidad para preservar la privacidad paneuropea (Pepp-Pt, 2020). Pero ese intento no fue bien visto por la ciudadanía y organismos no gubernamentales, quienes no vieron garantías de seguridad en estrategias centralizadas obligando al gobierno alemán a cambiar al enfoque Gapple.

En el mes de Junio, el laboratorio de seguridad de Amnistía internacional revisó las aplicaciones de rastreo de contactos de Europa, Oriente Medio y África del Norte encontrando que muchas de estas aplicaciones iban de malas a peligrosas para los derechos humanos, realizando seguimiento activo o casi en tiempo real de la ubicación de los usuarios mediante el Gps, además de la captura de datos susceptibles dirigidos a un servidor centralizado (Aministía internacional, 2020).

La ausencia de políticas internacionales para la protección de datos y la privacidad le han permitido a muchos gobiernos aprovecharse de los beneficios inmediatos generados por la crisis, minimizar las preocupaciones a largo plazo en relación a la inducción de tecnologías propias que facilitan la habituación a las políticas de seguridad. Además, de crear discriminación, desconfianza, problemas de salud por la ausencia de estudios de impactos previos y escenarios que exacerban la vulneración de derechos fundamentales en el mundo (Rowe, 2020; ServickMay, 2020; Zastrow, 2020).

La efectividad de estrategias de rastreo de contactos epidemiológicos mediante aplicativos móviles, según Rowe (2020) requieren 3 condiciones para que los aplicativos móviles sean efectivos:

1. debe garantizarse un alto número de pruebas de tamizaje y diagnósticas altamente sensibles y específicas, es decir con poca probabilidad de error;

2. debe garantizarse que en un encuentro entre un contagiado y un susceptible ambos posean un teléfono inteligente;

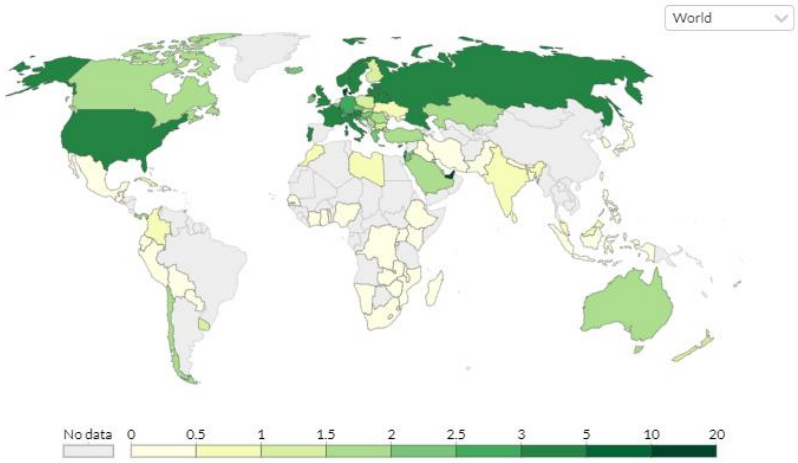
3. debe garantizarse que una proporción muy alta de usuarios de teléfonos inteligentes descargue la aplicación.

En relación a la condición número uno, ningún País conoce el número total de personas infectadas con Covid-19, solo se sabe el estado de infección de quienes se han sometido a la prueba, además ningún País realiza más de un millón de pruebas por semana. Al observar los datos estadísticos publicados semana a semana por la universidad de Oxford, sólo Emiratos Árabes Unidos, Dinamarca y Luxemburgo diez o más pruebas diarias por cada mil habitantes (Ritchie *et al*., 2020).

Para el caso de Colombia se realizan entre 02 y 0.45 pruebas diarias por cada mil habitantes, es decir diariamente se pueden realizar entre 20.000 a 45.000 mil pruebas (Editorial Dinero, 2020; Ritchie et al., 2020; Rueda, 2020), situación que impide controlar el nivel individual de patogenicidad del virus en un País de aproximadamente 50 millones de habitantes.

Pero este no es el único obstáculo, muchas de las pruebas rápidas realizadas en el Colombia particularmente tienen sensibilidad y especificidad muy bajas, esto varía entre las casas comerciales lo cual podría generar que en muchos sectores del País podrían circular muchos falsos negativos (aquellos casos que siendo positivos obtienen un resultado negativo), los resultados de la evaluación de estas pruebas fue realizada por el Instituto nacional de salud en los protocolos de validación de desempeño de pruebas rápidas Covid-19 IgG/IgM (Orozco *et al*., 2020).

Grafico 1 - Mapa de pruebas diarias de Covid-19 por cada mil personas, 18 de noviembre de 2020. Cifras promedio móvil de 7 días



Fuente: H. Ritchie, E. Ortiz-Ospina, D. Beltekian, E. Mathieu, J. Hasell, B. Macdonald, C. Giattino, M. Roser, Coronavirus (Covid-19). Testing-Statistics and Research. Our World in Data, 2020, https://ourworldindata.org/coronavirus-testing.

Respecto a la condición número dos, el País que implementa el rastreo de contactos a través de aplicaciones móviles debe garantizar que los ciudadanos poseen teléfonos inteligentes y que siempre lo porten. En el caso de Colombia, según el informe de indicadores de terminales por cada 100 habitantes hay 57.3 smartphones. Países como Australia, Francia, Alemania y otros de economías avanzadas que han reconocido la ineficiencia en el uso de estos aplicativos relacionados con la portabilidad de teléfonos inteligentes, poseen cifras de tenencia de smartphones de hasta 77 por cada 100 habitantes (Chugh, 2020; Rowe, 2020; Zastrow, 2020).

En cuanto a la condición número tres, una preimpresión de un grupo de la Universidad de Oxford, sugirió que la efectividad de estos aplicativos en el control del brote, requería aproximadamente una adherencia al uso del aplicativo por parte del 60% de la población (Fraser *et al*., 2020) situación imposible de cumplir teniendo en cuenta la situación de Colombia respecto a la portabilidad de teléfonos inteligentes en el País, a pesar de imponerse la descarga obligatoria.

En relación a los problemas de privacidad, una de las principales preocupaciones fue el almacenamiento de datos de los usuarios en servidores centralizados exponiendo a los usuarios a tráfico y piratería de datos y vigilancia relacionada con la vulnerabilidad y el monitoreo de la tecnología (Rowe, 2020).

De esta manera las aplicaciones para teléfonos inteligentes contra la epidemia de Covid-19 les han permitido a muchos gobiernos realizar bajo los criterios de Estados de excepción la recolección de datos de forma indiscriminada y con ello, es claro que dicho análisis en el caso colombiano es similar.

Por ello vale la pena resaltar, que bajo estos condicionamientos, la naturaleza del estado de excepción reglado constitucionalmente, las facultades que se le brindan al

gobierno nacional se encuentran dadas por un margen de competencias brindadas al ejecutivo cuya única limitación es la suspensión de derechos fundamentales, lo que nos lleva a determinar una análisis acucioso sobre los criterios jurídicos relevantes en el caso colombiano.

1. El estado constitucional, los derechos fundamentales y Medellín me cuida (App)

En este presupuesto, vale la pena resaltar entonces que, dentro de las condiciones estructurales del Estado Colombiano, es claro reconocer que, desde el planteamiento jurídico, las relaciones entre el Estado y los ciudadanos se regulan a través de las garantías constitucionales representadas en derechos fundamentales, las cuales se convierten en el núcleo del ordenamiento jurídico.

De esta dimensión, es claro que bajo el margen constitucional, el desarrollo de la constitución política de 1991, trae consigo no solo un ordenamiento jurídico que entiende las disposiciones formales en términos normativos, sino que entiende que el sistema normativo se debe al criterio de supremacía constitucional, y con ello comprende que la constitución política al determinar su carácter jerárquico, desarrolla un punto de relacionamiento entre el orden jurídico y las posibilidades de los servidores públicos que entran a reconocer, que bajo este principio el constitucionalismo revista una orientación que se convierte en un límite no solo en términos jurídicos sino también políticos (Roncancio, Restrepo, Colorado, 2020).

Por esta razón, al desarrollar los lineamientos de funcionamiento de la estructura del Estado, vale la pena entonces resaltar que, bajo esta dinámica, las normas jurídicas y las decisiones políticas hechas por quienes son los representantes de la ciudadanía bajo la condición del poder constituido, en su dimensión ejercen funciones públicas que deben reconocer las limitaciones que se les imponen desde la ley, pero a su vez desde la constitución. Lo que implica que incluso en los términos de una situación tan compleja como lo representa la pandemia del coronavirus, la misma está sujeta a los criterios desarrollados en materia de derechos fundamentales por el sistema jurídico.

Lo anterior, conforme destaca la profesor Tobón (2019) implica un reconocimiento que en términos constitucionales, establece una limitación de orden formal y material, para que incluso en los denominados estados de excepción, los poderes exorbitantes de los cuales se dota al poder ejecutivo con la finalidad de establecer mecanismos de resolución política a las causas que alteran al orden social, tienen que prever un sistema de *check and balance*, que frena la actividad estatal en razón al respeto de los derechos fundamentales.

De modo tal, que frente a lo anterior, vale la pena entonces resaltar que cuando se plantea el reconocimiento de las variables con las que se generaron las medidas de adopción e implementación de medidas excepcionales, tiene que reconocerse que bajo este presupuesto existen condicionales que determinar i) los limites materiales que se crean en la actividad política alrededor de los derechos fundamentales y ii) los efectos

que se generan de una descuidada implementación de estas medidas en materia de derechos fundamentales alrededor de la implementación de los mismos.

Es preciso advertir entonces, que, pese a que existen buenas intenciones para establecer las medidas de equiparación y respuesta del uso de las aplicaciones para el manejo de información, las mismas han generado prácticas que han expuesto los riesgos del uso indebido de los datos de los usuarios. Esto ha implicado un problema importante en cuanto a que cada vez más esferas personales se han visto absorbidos por estos medios que facilitan el registro y el almacenamiento de datos personales que antes no eran intervenidos por la tecnología. Es decir, cada vez hay más bases de datos que contienen información cada vez más íntima de las personas.

Además, se determina que la recopilación de información, no solo puede tener una finalidad, sino que se puede presentar una utilización con variables diferenciales que aprovechan un mismo dato, con lo que se determina el inminente riesgo puesto que existen «algoritmos sofisticados para descubrir principalmente patrones ocultos, asociaciones, anomalías, y/o estructuras de la gran cantidad de datos almacenados en los data *warehouses* u otros repositorios de información» (Karina, Ruiz, Riquelme, 2006: 12).

En el caso específico de la pandemia actual, diferentes gobiernos del mundo han utilizado la minería de datos con la finalidad de analizar mejor el comportamiento del virus, y así combatirlo con mayor eficacia. Situación que no ha sido diferente en Colombia en donde se creó la aplicación Coronapp a nivel nacional, Medellín me cuida en la ciudad de Medellín, Calivallecorona en la ciudad de Cali y Gabo en la ciudad de Bogotá. Todas estas aplicaciones buscan combatir el coronavirus mediante la creación de grandes bases de datos de los ciudadanos y georreferenciación en tiempo real, y el análisis de esta información a través de la inteligencia artificial.

En el caso de Medellín me cuida el alcalde de Medellín Daniel Quintero Calle al presentar esta plataforma, expreso que

> en Medellín estamos tomando decisiones para enfrentar el coronavirus. Hoy tener información de cada familia, saber dónde está ubicada, cuántas personas viven, sus edades y su estado de salud es fundamental para ganar esta batalla. Por eso hemos creado Medellín me cuida, una plataforma que utiliza inteligencia artificial analítica de datos y Big data para poder enfrentar al coronavirus (@quinterocalle, 2020).

Dando cuenta que, frente a su implementación, se entiende que la misma tiene por propósito crear medidas efectivas para la atención de los datos generando mapeos epidemiológicos, y con ello medidas de intervención estatal para garantizar medidas de reducción y control de la expansión del virus. No obstante, desde el momento de su implementación, la utilización de la plataforma despertó inquietudes en la medida que solicitaba datos que caracterizaban a las personas más allá de las condiciones necesarias para su finalidad.

Ello se evidenciaba en los datos que se solicitaban concernientes a la conformación del grupo familiar, identidad sexual, población, lo que determino acciones judiciales en contra del uso de la app, y con ello la determinación de que ella tenía sobre la incidencia

de otros derechos fundamentales, en donde claramente, dicha situación refiere un estudio más acucioso sobre los elementos que deben considerarse.

En este presupuesto como condición del ordenamiento jurídico, los derechos de información, así como el tratamiento de los mismos, implica no solo una determinación sobre la órbita de la intimidad de los ciudadanos, sino que refiere sobre las condiciones de limitación del poder estatal en cuanto relacionan un direccionamiento sobre la esfera de las libertades y las condiciones autónomas de los ciudadanos frente a su libertad.

Por ello, es claro que, en nuestro ordenamiento jurídico, el habeas data es un derecho fundamental que busca proteger los datos personales de cualquier persona que reposen en bases de datos, ya sea de instituciones públicas o de particulares; salvo ciertas excepciones consagradas en la ley. El concepto de "base de datos" es definido por la corte constitucional como un «conjunto sistematizado de información personal que puede ser tratada de alguna manera, como ocurre con el ejercicio de los atributos de recolección, uso, almacenamiento, circulación o supresión» (Corte constitucional, 2014: 14). Este derecho fundamental se encuentra consagrado en el artículo 15 de la constitución política. Aunque se encuentra en el mismo artículo del derecho a la intimidad, el habeas data es un derecho fundamental autónomo, y está desarrollado en la ley estatutaria n.1581 de 2012 sobre las disposiciones generales para la protección de datos personales. Esta, establece los principios generales y reglas mínimas que deben ser acatadas por las instituciones que poseen bases de datos de cualquier naturaleza; establece los alcances de este derecho fundamental, así como los procedimientos para acceder a su tutela a través de la Superintendencia de industria y comercio.

Según este estatuto, los principios rectores que se deben observar a la hora de recolectar, usar, almacenar, transmitir o realizar cualquier tipo de tratamiento sobre datos personales, son los siguientes:

a. principio de legalidad. Este principio establece como regla general que todo tratamiento de datos personales debe acatar las reglas básicas establecidas en las normas;

b. principio de finalidad. Establece que la finalidad que motive cualquier tratamiento de datos personales debe estar dentro del marco constitucional y legal, y debe ser expresada al titular antes de realizar cualquier tratamiento sobre sus datos personales. La Corte ha interpretado este principio como «la exigencia de someter la recopilación y divulgación de datos, a la realización de una finalidad constitucionalmente legítima, lo que impide obligar a los ciudadanos a relevar datos íntimos su vida personal, sin un soporte en el texto constitucional que, por ejemplo, legitime la cesión de parte de su interioridad en beneficio de la comunidad» (Corte constitucional, 2004: 28);

c. principio de libertad. Establece que para que cualquier entidad pueda realizar el tratamiento de los datos personales de cualquier persona, es un requisito esencial el consentimiento previo, expreso e informado de éste. También establece que la excepción para obtener, almacenar o transmitir la información personal de alguien sin su consentimiento, es cuando medie una orden judicial o un mandato legal. Para la Corte, este principio es «el pilar fundamental de la administración de datos», pues es

una condición esencial para la legalidad de cualquier actividad de tratamiento de datos personales, sean sensibles o no (Corte constitucional, 2011: 188)

d. principio de veracidad. Establece que la información personal objeto de tratamiento debe ser completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

e. principio de transparencia. Otorga la facultad al titular de acceder en cualquier momento y sin restricciones, a la información personal que repose en cualquier base de datos;

f. principio de acceso y circulación restringida. Los datos deben ser administrados de conformidad a una política rigurosa que impida que se puedan afectar derechos fundamentales;

g. principio de seguridad. En este principio la corte establece que «se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento» como se plantea en la ley estatutaria 1581 de 2012 (Ley estatutaria de 2012, articulo 4 literal g);

h. principio de confidencialidad Según este principio, las entidades que administren bases de datos deben garantizar la reserva de la información.

Por otra parte, esta ley define el concepto de datos sensibles, y establece como regla general la prohibición del tratamiento de esta categoría especial de datos; es decir, la prohibición de su recolección, uso, almacenamiento y circulación. Define los datos sensibles como aquellos «que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos» (ley estatutaria 1581 de 2012, articulo 5).

De modo tal que, bajo una visión hermenéutica, implica reconocer que bajo estos criterios, la dinámica de interpretación que se genera sobre los datos se encuentra sujeto a criterios de interpretación, que en todo caso, estarán ligados a que dentro de su operación, la obtención de datos, su tratamiento y la disposición de los mismos están ligados a una condición de ser tratados como derecho fundamental.

Ello, entonces, determina que el margen de regulación específica que se deriva de las condiciones propias de los síntomas y la prevención de la generación de casos articulada con las medidas de detección, que en todo caso, dependen de factores objetivos que no son propios a su margen de aplicación, y que en consecuencia depende de la legitimidad que se construye de las decisiones tomadas por la institucionalidad.

En este propósito, es claro, que la finalidad constitucionalmente perseguida es válida, en tanto establece una fórmula de intervención orientada a proteger derechos fundamentales, y con este propósito, el objeto de la misma entiende que su utilización se encuentra justificada en el reconocimiento de una pandemia. No obstante, es claro afirmar que en ese direccionamiento el último límite que se genera está articulado a los

derechos fundamentales que bajo ningún criterio pueden suspenderse ni siquiera en un Estado de excepción.

En este punto es claro, que la determinación de la aplicación del uso del aplicativo, Medellín me cuida, luego entonces tiene una determinación que debe ser ponderada bajo tres márgenes específicos, los cuales son tenidos y desarrollados conforme a su determinación estructural en la medida que i) son relevantes para determinar la incidencia de gobierno, ii) respetan las condiciones propias a las del fin constitucionalmente valido, iii) desarrollan un criterio amplio sobre la toma decisiones inherentes al estado de emergencia.

2. Limitaciones al uso de la información en el caso de Medellín

Bajo este criterio, es claro que luego entonces no se puede dar uso de la información de forma indiscriminada a una limitación, de orden formal fijada en términos de derechos fundamentales, en tanto su concreción está ligada al cumplimiento de las disposiciones legales. En la ley de protección de datos se imponen diversas obligaciones a los responsables y encargados del tratamiento de datos personales, y se dispone que todas las entidades que realicen actividades relacionadas con la administración de datos personales, están obligadas a «adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley, y en especial, para la atención de consultas y reclamos» (Congreso de Colombia, 2012: articulo 17 literal k). Además, se impone la obligación de registrar estos manuales en el Registro nacional de bases de datos para asegurar su legalidad, y se conmina a los responsables y encargados del tratamiento de datos personales a respetar estas políticas, que en ningún caso pueden establecer garantías menores a las establecidas en la legislación.

La norma encargada de regular el marco general de protección de datos, es el decreto n.1377 de 2013, por medio de la cual se reglamenta parcialmente la ley n.1581 de 2012. Esta establece las reglas que deben observar las entidades a la hora de elaborar una política de tratamiento de datos personales (recolección, análisis, almacenamiento, transferencia, supresión), y establece el principio de responsabilidad demostrada. Según este principio, los encargados de administrar bases de datos deben ser capaces de «demostrar, a petición de la Superintendencia de industria y comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley n.1581 de 2012 y este decreto» (Decreto n.1377 de 2013, articulo 26).

Por otra parte, en Colombia se implementa un modelo hibrido de protección de datos personales, por lo cual existen múltiples normas sectoriales que pueden reglamentar el tratamiento de datos personales, en concordancia con la ley general, a través de actos administrativos por parte de las entidades territoriales o del gobierno nacional.

En el caso de la alcaldía de Medellín, el decreto n.1096 de 2018, por medio del cual se adopta la politica para el tratamiento de datos personales en el municipio de Medellín, prescribe que toda información que repose en las bases de datos de sus

dominios puede ser empleada por la alcaldía, sin limitaciones, para el ejercicio de todas sus competencias funcionales[1].

Por otra parte, establece que la forma de obtención de la información personal es «el suministro voluntario y directo por sus titulares, a través de contacto personal, llamadas telefónicas, página de internet, celebración de contratos, eventos o correos electrónicos»[2].

Para el caso específico de la plataforma Medellín me cuida, existe un manual de términos y condiciones para el uso de la plataforma, pero no es exclusivo, sino que cohabita con el decreto anteriormente citado, por lo cual los datos personales que almacena esta plataforma son tratados bajo las premisas establecidas en ambos manuales para el tratamiento de datos personales.

El manual de términos y condiciones establece que:

Quinta - Tratamiento de datos personales. A través del formulario de la plataforma Medellín me cuida-familias recolecta datos públicos, semiprivados, privados y sensibles de los usuarios, los cuales serán tratados por la alcaldía de Medellín para el despliegue de medidas de prevención, contención, atención y mitigación frente a los impactos ocasionados por el virus del Covid-19 y las medidas adoptadas, específicamente para: (i) crear y activar el registro de usuario en Medellín me cuida-familias; (ii) permitir al usuario el ingreso a Medellín me cuida-familias y el diligenciamiento del formulario; (iii)diligenciamiento del formulario con la información privada, semiprivada y pública; (iv)acceder a la geolocalización de usuarios de acuerdo a la información proporcionada para despliegue de esfuerzos de tratamiento de los impactos ocasionados con la emergencia, (v)atender las finalidades que persigue la plataforma y el formulario. Los datos suministrados serán tratados conforme a lo dispuesto en la ley n.1581 de 2012, sus decretos reglamentarios y el decreto n.1096 de 2018 de la alcaldía de Medellín.

En este sentido, se evidencia que a pesar de comenzar afirmando que los datos sensibles, privados, semi privados y públicos serán tratados para tomar medidas en contra del Covid-19, al final del mismo párrafo deja la puerta abierta para aplicar el decreto n.1096 de 2018, el cual permite a la alcaldía utilizar la información de sus bases de datos sin más limitación que el cumplimiento de sus funciones legales, lo cual vulnera el principio de finalidad.

Además, la política de términos y condiciones de Medellín me cuida faculta expresamente a la alcaldía a trasferir estos datos de forma anonimizada a entidades de

[1] «*II. Finalidad del tratamiento de los datos personales* - La información suministrada por el Titular será incluida en las bases de datos del Municipio de Medellín para llevar a cabo acciones relacionadas con sus funciones legales y su objeto misional, lo que comprende todas sus competencias funcionales incluyendo, sin limitación, todos los trámites, gestiones, servicios, consultas, notificaciones, registros, ente otros, que se requiera realizar en virtud de la relación que se tenga o establezca con éste y de acuerdo con el tipo de base de datos en la que se encuentre incluido y el objeto específico de la misma. Igualmente, con el fin de brindar un excelente servicio a todos los usuarios, para dar efectivo cumplimiento a todas las obligaciones legales y contractuales y para lograr relaciones más efectivas, agiles y seguras con los diferentes Titulares de datos personales».

[2] «*IV. Forma en la cual se obtienen los datos personales* - Los datos personales que obtiene y almacena el Municipio de Medellín, son suministrados voluntaria y directamente por sus Titulares, a través de contacto personal, Llamadas telefónicas, página de internet, celebración de contratos, eventos o correos electrónicos».

salud, transferencias que pueden ser interferidas por terceras personas, lo cual plantea un reto en cuanto a la seguridad y confidencialidad de los datos personales.

Dejando claro que en el caso de Colombia esta limitación supone una grave afectación con los criterios jurídicos que se han construido dentro del ordenamiento jurídico. En este criterio es nominalmente valido que se puedan utilizar este tipo de aplicaciones, no obstante, es necesario que se delimite claramente conforme los criterios de interpretación constitucional su utilización.

En todo caso, los actos administrativos en Colombia se encuentran sujetos al principio de supremacía constitucional, y en dicho propósito la afectación de los márgenes de los manejos de datos e información solo es posible cuando su finalidad corresponde a la suspensión de derechos fundamentales.

El criterio discrecional luego entonces bajo ningún supuesto faculta al mandatario local, a utilizar de forma indiscriminada la crisis para obtener datos diferentes a los realmente relevantes para conjurar la pandemia, que en este caso están ligados a síntomas y condiciones propias de núcleos que puedan ser significativos para afrontar la pandemia producida en el marco de una emergencia de salud pública.

Puesto que, de vulnerarse estos criterios, es claro que su utilización implica una ruptura al orden constitucional y en dicha determinación, determinaría que las actuaciones posteriormente dadas puedan determinar acciones de orden legal por un indebido uso de información. Bajo estos criterios para su obtención esta debe generarse sobre una irreductible condición, la cual determina la pertinencia, la necesidad y la relevancia de los datos con el objeto de la calamidad pública, puesto que, de otra condición, ello implicaría una política arbitraria.

Finalmente vale resaltar que los márgenes de intervención estatal que se encuentran fijados en el estado social de derecho solo estiman como posible la intervención que se hace para garantizar de forma más amplia los derechos fundamentales, y que bajo esta dinámica no se puede determinar una lesividad de los mismos bajo la disposición de un estado de excepción, pues es claro que i) en Colombia los estados de excepción tienen condiciones de regulación especiales que impiden la limitación de derechos fundamentales y ii) los criterios de conexidad y relevancia están dados para la obtención de datos clínicos que generen legitimidad y confianza sobre la ciudadanía. Puesto que de presentarse la ausencia de uno de estos elementos terminarían generando un fracaso en la política de prevención de esta y de otras situaciones en futuro.

Referencias bibliográficas / References

Alcaldia de Medellin, *Decreto n.1096*, 2018, en https://www.medellin.gov.co/normograma/docs/d_alcamed_1096_2018.htm, consultado el 7 de octubre de 2020.

Aministía internacional, *Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy*, 2020, en https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/, consultado el 8 de septiembre de 2020.

Asomóvil, *Uso de los smartphones en Colombia ya es mayor al 50% de la población, según Asomóvil*, 2017, en http://www.asomovil.org/uso-de-los-smartphones-en-colombia-ya-es-mayor-al-50-de-la-poblacion-segun-asomovil/, consultado el 9 de septiembre de 2020.

Casa editorial el Tiempo, *Número de celulares inteligentes en el País aumentó 50% en el último año*, «Portafolio.co», 2017, en https://www.portafolio.co/tendencias/tenencia-de-smartphones-aumento-50-en-colombia-en-el-2016-505967, consultado el 9 de septiembre de 2020.

Chan A.K.M., Nickson C.P., Rudolph J.W., Lee A., Joynt G.M., *Social Media for Rapid Knowledge Dissemination. Early Experience from the Covid-19 Pandemic*, «Anaesthesia, 2020.

Chugh R., *Why Australia Should Consider Ditching CovidSafe in Favour of Gapple*, «Lifehacker», 2020, en https://www.lifehacker.com.au/2020/07/why-australia-should-consider-ditching-covidsafe-in-favour-of-gapple/, consultado el 8 de septiembre de 2020.

Congreso de la Republica de Colombia, *Ley estatutaria n.1581 de 2012*, 2012, en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html, consultado el 28 de agosto de 2020.

Congreso de la Republica de Colombia, *Ley n.1581*, 2012, en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html,_consultado el 8 de septiembre de 2020.

Corte constitucional, *Sentencia n.C748 de 2011*, M.P Jorge Ignacio Pretel, 2011, en https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm, consultado el 29 de agosto de 2020.

Corte constitucional, *Sentencia n.T020 de 2014*, M.P Luis Guillermo Guerrero, 2014, en https://www.corteconstitucional.gov.co/relatoria/2014/T-020-14.htm, consultado el 29 de agosto de 2020.

Corte constitucional, *Sentencia n.T787 de 2004*, M.P Rodrigo Escobar Gil, 2002, en https://www.corteconstitucional.gov.co/relatoria/2004/t-787-04.htm, consultado el 8 de septiembre de 2020.

Editorial Dinero, *¿Por qué bajó el número de pruebas de covid19 en Colombia?*, 2020, http://www.dinero.com/pais/articulo/por-que-bajo-el-numero-de-pruebas-de-covid-19-en-colombia/297494, consultado el 8 de septiembre de 2020.

Edwards J., *Tracking Coronavirus: Should you Install the CoronApp?*, «The Bogotá Post», 19 de junio, 2020, en https://thebogotapost.com/tracking-coronavirus-coronapp/46864/, consultado el 29 de agosto de 2020.

Elmer T., Mepham K., Stadtfeld C., *Students under Lockdown: Comparisons of Students' Social Networks and Mental Health Before and During the Covid-19 Crisis in Switzerland*, «Plos One», 15(7), 2020.

European Consortium, *Decentralized Privacy-Preserving Proximity Tracing* [Shell], DP-3T, en https://github.com/DP-3T/documents, Original work published 2020, consultado el 7 de septiembre de 2020.

Fahey R.A., Hino A., *Covid-19. Digital Privacy and the Social Limits on Data-Focused*

Public Health Responses, «International Journal of Information Management», 102181, 2020, en https://doi.org/10.1016/j.ijinfomgt.2020.102181, consultado el 27 de agosto de 2020.

Fraser C., Abeler-Dörner L., Ferretti L., Parker M., Kendall M., Bonsall D., *Digital contact tracing: Comparing the capabilities of centralised and decentralised data architectures to effectively suppress the Covid-19 epidemic whilst maximising freedom of movement and maintaining privacy*, 2020, en https://go.nature.com/2x2czk9, consultado el 7 de septiembre de 2020.

Freitas A.R.R., Napimoga M., Donalisio M.R., Freitas A.R.R., Napimoga M., Donalisio M.R., *Análise da gravidade da pandemia de Covid-19*, «Epidemiologia e Serviços de Saúde», 29(2), 2020.

Gvili Y., *Security Analysis of the Covid-19 Contact Tracing Specifications by Apple Inc. And Google Inc.*, n.428, 2020, en http://eprint.iacr.org/2020/428, consultado el 8 de septiembre de 2020.

Infometrika, *Diseño y medición, Indicador Terminales por cada 100 habitantes. En el marco del Plan nacional de desarrollo 2014-2018*, Ministerio de tecnologias de la información y las telecomunicaciones, 2016, en https://www.mintic.gov.co/portal/604/articles-51641_recurso_1.pdf, consultado el 10 de septiembre de 2020.

Leite H., Hodgkinson I.R., Gruber T., *New Development. 'Healing at a Distance' - Telemedicine and Covid-19*, «Public Money & Management», 40(6), 2020, pp.483-485.

Lincoln H., Khan R., Cai J., *Telecommuting: A Viable Option for Medical Physicists Amid the Covid-19 Outbreak and Beyond*, «Medical Physics», 47(5), 2020, pp.2045-2048.

Marroquín B., Vine V., Morgan R., *Mental Health during the Covid-19 Pandemic. Effects of Stay-at-Home Policies, Social Distancing Behavior, and Social Resources*, «Psychiatry Research», 293, noviembre, 2020.

Martin R.D., (2020) *Leveraging Telecommuting Pharmacists in the post Covid-19 World*, «Journal of the American Pharmacists Association», 60(6), 2020.

Michael K., Abbas R., *Behind Covid-19 Contact Trace Apps. The Google-Apple Partnership*, «Ieee Consumer Electronics Magazine», 9(5), 2020, pp.71-76.

Mintic-Ministerio de tecnologías de la información y las comunicaciones, *Tenencia de smartphones aumentó 50% en Colombia en el 2016-Tenencia de smartphones aumentó 50% en Colombia en el 2016*, Mintic, diciembre de 2016, Bogotá, en http://www.mintic.gov.co/portal/604/w3-article-51641.html, consultado el 9 de septiembre de 2020.

Ni M.Y., Yang L., Leung C.M.C., Li N., Yao X.I., Wang Y., Leung G.M., Cowling B.J., Liao Q., *Mental Health, Risk Factors, and Social Media Use during the Covid-19 Epidemic and Cordon Sanitaire among the Community and Health Professionals in Wuhan, China. Cross-Sectional Survey*, «Jmir. Mental Health», 7(5), 2020.

Orozco K.E., Robayo A., Arévalo A., Zabaleta G., *Protocolo de validación secundaria de desempeño de pruebas rápidas Covid-19 IgG/IgM*, Instituto nacional de salud, 2020, en https://www.ins.gov.co/Pruebas_Rapidas/2.%20Protocolo%20Est%C3%A1ndar%20para%20validaci%C3%B3n%20de%20PR%20en%20Colombia.pdf, consultado el 9 de

septiembre de 2020.
Ortega G., Rodriguez J.A., Maurer L.R., Witt E.E., Perez N., Reich A., Bates D.W., *Telemedicine, Covid-19, and disparities: Policy implications*, «Health Policy and Technology», 9(3), 2020.
Pact's, *Pact: Rastreo de contactos automatizado privado*, 2020, https://pact.mit.edu/, consultado el 8 de septiembre de 2020.
Pappot N., Taarnhøj G.A., Pappot H., *Telemedicine and e-Health Solutions for Covid-19. Patients' Perspective*, «Telemedicine and e-Health», 26(7), 2020.
Pepp-Pt, *Pan-European Privacy-Preserving Proximity Tracing Pepp-Pt*, Pepp Pt, 2020, en https://www.pepp-pt.org, consultado el 8 de septiembre de 2020.
Quintero Calle D. @quintero calle, *#MedellínMeCuida es la estrategia más poderosa de información para enfrentar al coronavirus y, a la vez, atender a la población más vulnerable. Con ella podemos actuar a tiempo. Cada familia de Medellín debe inscribirse*, Twitter, 5 de abril de 2020, en https://twitter.com/quinterocalle/ status/1246909321847410692, consultado el 26/08/2020.
Riquelme J.C., Ruiz R., Gilbert K., *Minería de datos. Conceptos y tendencias. Inteligencia artificial*, «Revista Iberoamericana de Inteligencia Artificial», 10(29), 2006, pp.11-18.
Ritchie H., Ortiz-Ospina E., Beltekian D., Mathieu E., Hasell J., Macdonald B., Giattino C., Roser M., *Coronavirus (Covid-19). Testing-Statistics and Research. Our World in Data*, 2020, en https://ourworldindata.org/coronavirus-testing, consultado el 19 de noviembre de 2020.
Roncancio A., Restrepo F., Colorado S., *La supremacía constitucional en el Estado social de derecho*, «Ratio Iuris», 15(31), 2020, pp.189-204.
Rowe F., *Contact Tracing Apps and Values Dilemmas. A Privacy Paradox in a Neo-Liberal World*, «International Journal of Information Management», 55, 21 de diciembre, 2020.
Rueda J.P., *Así va Colombia en pruebas para detectar Covid-19*, «El Tiempo», 13 de agosto, 2020.
Servick K., *Covid-19 Contact Tracing Apps Are Coming to a Phone near You. How Will We Know Whether They Work?*, «Science - Aaas, Technology and Coronavirus», 21 de mayo, 2020.
Sugestyo Putro S., Riyanto S., *How Asian Sandwich Generation Managing Stress in Telecommuting during Covid-19 Pandemic*, «International Journal of Scientific Research and Engineering Development», 3(3), 2020, pp.485-492.
Tobon M., *Los estados de excepción. Imposibilidad de suspensión de los derechos humanos y las libertades fundamentales*, Grupo Editorial Ibañez, Bogotá, 2019.
Torok M., *Rastreo de contactos*, «Focus on Field Epidemiology», 4(6), 2005, pp.1-5.
TraceTogether, *TraceTogether*, 2020, https://www.tracetogether.gov.sg, consultado el 8 de mayo de 2020.
Verhagen L.M., de Groot R., Lawrence C.A., Taljaard J., Cotton M F., Rabie H., *Covid-19 Response in Low - and Middle - Income Countries. Don't Overlook the Role of*

Mobile Phone Communication, «International Journal of Infectious Diseases», 99, 2020, pp.334-337.

Zastrow M., *Coronavirus Contact-Tracing Apps: Can They Slow the Spread of Covid-19?*, «Nature», 19 de mayo, 2020.

Recibido: 12/09/2020
Aceptado: 7/12/2020