



# Discusión en redes sociales sobre el rastreo digital de contactos para COVID-19: retos para la salud pública desde Colombia\*

## Discussions on social media about digital contact tracing for COVID-19: Challenges for public health from Colombia

### Discussão em redes sociais sobre o monitoramento digital de contatos para COVID-19: desafios para a saúde pública da Colômbia

**Recibido:** 30 de Noviembre de 2020. **Aceptado:** 17 de Marzo de 2021.  
**Publicado:** 30 de diciembre de 2021.

DOI: <https://doi.org/10.11144/Javeriana.rgps20.drsr>

Sandra Milena Agudelo Londoño<sup>a</sup>  
Pontificia Universidad Javeriana, Colombia  
ORCID: <https://orcid.org/0000-0002-8980-6590>

Clara Andrea Núñez Avilés  
Pontificia Universidad Javeriana, Colombia  
ORCID: <https://orcid.org/0000-0001-6515-9504>

**Para citar este artículo** Agudelo-Londoño SM, Núñez CA. Discusión en redes sociales sobre el rastreo digital de contactos para COVID-19: retos para la salud pública desde Colombia. Rev Gerenc Polit Salud. 2021;20. <https://doi.org/10.11144/Javeriana.rgps20.drsr>

---

\* Artículo de investigación

<sup>a</sup> Autora de correspondencia. Correo electrónico: [sandra.agudelo@javeriana.edu.co](mailto:sandra.agudelo@javeriana.edu.co)



## Resumen

**Introducción.** Aunque las pandemias no son un fenómeno nuevo para la humanidad, la pandemia por COVID-19 trae consigo preocupaciones inéditas que ameritan una lectura atenta, en especial en lo relacionado con el rastreo digital de contactos. **Métodos.** Entre marzo y septiembre de 2020 se realizó una etnografía digital con el fin de caracterizar las aplicaciones móviles creadas en Colombia para el rastreo digital de contactos por la pandemia de COVID-19. Se hizo énfasis en la aplicación CoronApp respaldada por el gobierno nacional y se realizó un análisis de la discusión ciudadana sobre estas intervenciones en las redes sociales. **Resultados.** Se identificaron 16 tecnologías para COVID-19 entre aplicaciones móviles para el rastreo y aplicativos web para el control de actividades laborales, sociales o de movilidad. La aplicación CoronApp tenía más de 10 millones de descargas y el uso más extendido en el país. Las preocupaciones de los usuarios fueron frecuentes, en especial frente a las pocas garantías de confidencialidad en el manejo de los datos, la invasión a la privacidad, el riesgo de mercantilización, el poder del Estado y el rol de los derechos ciudadanos digitales, así como la poca claridad en la política epidemiológica detrás de las aplicaciones. **Discusión.** La pandemia de COVID-19 es el primer evento global que se combate digitalmente, lo que significa un nuevo universo de posibilidades para la salud pública, pero también, retos sociales y ciudadanos sobre el gobierno de la salud y la vida que no deben pasarse por alto.

**Palabras clave:** COVID-19, vigilancia en salud pública, vigilancia epidemiológica, sistema de vigilancia sanitaria.

## Abstract

**Introduction.** Pandemics are not a new phenomenon for humanity. COVID-19 pandemic brings unprecedented concerns that merit a careful reading, especially regarding digital contact tracing. **Methods.** A digital ethnography was carried out between March to September of 2020 to characterize the mobile applications created in Colombia for COVID-19 digital contact tracing. Emphasis was put on CoronApp, supported by the national government, leading to an analysis of citizens' discussions about these interventions on social networks. **Results.** Sixteen technologies for COVID-19 were identified, among mobile tracing applications and internet applications for labor, social, and mobility monitoring. The CoronApp application had more than 10 million downloads and it was the most used in the country. Users concerns were frequent, especially apropos the lack of guarantees of confidentiality in the handling of data, invasion of privacy, risk of commercialization, the power of state, the role of digital citizens' rights, as well as the lack of clarity on the epidemiological policy behind the apps. **Discussion.** The COVID-19 pandemic is the first global event to be fought digitally. That means a world of possibilities for public health but social and civic challenges about the governance of health and life, as well.

**Keywords:** COVID-19, public health monitoring, epidemiological monitoring, health monitoring system.

## Resumo

**Introdução.** Embora as pandemias não sejam um fenômeno novo para a humanidade, a pandemia pela COVID-19 traz consigo preocupações inéditas que merecem uma leitura cuidadosa, especialmente em relação ao monitoramento digital de contatos. **Métodos.** Entre março e setembro de 2020, foi realizada uma etnografia digital a fim de caracterizar os aplicativos móveis criados na Colômbia para monitoramento digital de contatos devido à pandemia da COVID-19. Foi enfatizado o aplicativo CoronApp, respaldado pelo governo nacional; tornando-se uma análise da discussão cidadã sobre essas intervenções nas redes sociais. **Resultados.** Foram identificadas 16 tecnologias para a COVID-19 entre aplicativos móveis para monitoramento e aplicativos web para controle de atividades laborais, sociais ou de mobilidade. O aplicativo CoronApp tinha mais de 10 milhões de downloads e o uso mais difundido no país. As preocupações dos usuários foram frequentes, principalmente quanto às poucas garantias de sigilo na utilização dos dados, a invasão de privacidade, o risco de comercialização, o poder do Estado e o papel dos direitos digitais do cidadão, bem como a falta de clareza na política epidemiológica por trás dos aplicativos. **Discussão.** A pandemia da COVID-19 é o primeiro evento global a ser combatido digitalmente, o que significa um novo universo de possibilidades para a saúde pública, mas também desafios sociais e cidadãos quanto à governança da saúde e da vida que não devem ser esquecidos.

**Palavras-chave:** COVID-19, vigilância em saúde pública, vigilância epidemiológica, sistema de vigilância em saúde.



## Introducción

Aunque las pandemias no son un fenómeno nuevo para la humanidad, esta pandemia por COVID-19 (1) carga consigo preocupaciones inéditas que, situadas en este momento histórico, ameritan una lectura atenta a las posibilidades y retos de hacer salud pública desde lo digital (2). Una de estas estrategias digitales, de interés para este trabajo, es el rastreo digital de contactos (3).

El rastreo digital es la adaptación contemporánea de una práctica epidemiológica con importante tradición en el campo: el rastreo físico de contactos (2). Esta técnica junto con las cuarentenas (4), el lavado de manos (5) y el uso de las máscaras faciales o tapabocas (6) (en el caso de las infecciones respiratorias), han sido las principales estrategias para la contención de las enfermedades transmisibles que afectan a las sociedades actuales, junto con el desarrollo biomédico de las vacunas, los medicamentos y los antibióticos (7).

Desde finales del siglo XIX, se pueden rastrear experiencias de lo que hoy se denomina rastreo de contactos como respuesta de las autoridades para la contención de las enfermedades infectocontagiosa, como la viruela (8) y la peste bubónica (9). Esta práctica ha evolucionado bajo la idea de que estas enfermedades se propagan a través de cadenas de transmisión, de manera que con la identificación de las personas que han estado en contacto con enfermos, se pueden cortar las cadenas. Su aplicación es habitual en la epidemiología de enfermedades infecciosas como la tuberculosis, el VIH/Sida y otros eventos de transmisión sexual (10).

La modalidad digital del rastreo de contactos surgió en 2015 como práctica en la epidemia del síndrome respiratorio de Oriente Medio (MERS-CoV) (3), pero su utilidad se identificó hace pocos años más, a principios del siglo XXI, para la notificación de parejas en el caso de sífilis (una técnica de rastreo para infecciones sexuales) (11) o para el rastreo de la gripe en Reino Unido en 2010, con experiencias como FluPhone (12). En ese sentido, el rastreo digital de contactos es una práctica antigua vestida con nuevo ropaje. El proceso se basa en el uso de los dispositivos móviles personales, redes sociales, sistemas de posicionamiento o satélites para rastrear, desde la cuenta de una persona contagiada, a todos los posibles contactos que ha tenido en un periodo de tiempo y aislarlos o tratarlos según necesidad (13).

Para la salud pública contemporánea el uso de tecnologías digitales que ayuden a mejorar procesos de promoción, atención en salud y prevención de la enfermedad es una práctica creciente y parece deseable. En especial, la epidemiología ha acuñado ya varias expresiones para el aprovechamiento de los datos digitales en las acciones de vigilancia, como la *infodemiology* o *la infoveillance* (14,15). Esta tendencia sin embargo, se ha caracterizado por una visión acrítica de las posibles consecuencias no deliberadas de la tecnología sobre la salud y la vida, además de una falta de reflexión sobre el alcance, los límites en el diseño y el uso de estas tecnologías, de cara al rol de la salud pública (16). Esto es especialmente relevante en épocas de crisis sociales, económicas y sanitarias como las que acontecen en una pandemia.

El rastreo de contactos para COVID-19 se ha dado en el marco de declaraciones de estados de excepción en muchos países y territorios, y ha sido promovido como uno de los pilares para el control de la infección (17,18). A noviembre de 2020, el proyecto ‘rastreador de rastreadores’ de COVID-19 del *Massachusetts Institute of Technology* ha identificado 25 países que utilizan estrategias de rastreo digital de contactos para COVID-19 a escala nacional (17,19). Colombia aún no aparece en sus registros y México es el único país suramericano incluido en la lista. En ese sentido, es evidente que la carrera tecnológica de la sociedad contemporánea ha llevado a las autoridades sanitarias a promover y/o crear incontables estrategias de rastreo e identificación de contagiados, como aplicaciones móviles, sistemas de vigilancia por cámaras (20), por geoubicación (21) o por redes sociales, entre otras (22).

Esta proliferación de prácticas de vigilancia digital ha estado acompañada de la expresión ciudadana de preocupaciones sobre asuntos como la privacidad, la seguridad y las libertades individuales en el marco de los regímenes políticos (23). Asimismo, se han puesto en la discusión pública el rol y alcance de las acciones en salud pública y de las agencias sanitarias sobre el gobierno de la vida (19). Todo esto porque hay ciertas semejanzas, sobre todo en la base tecnológica y en el desconocimiento general del público, entre la vigilancia para la salud pública y aquella para la seguridad nacional (2). En contextos tan politizados y de desconfianza con las autoridades gubernamentales –como el caso de Colombia– (24), las alarmas de la ciudadanía sobre el uso de sus datos no se hacen esperar.

En Colombia existe un notable incremento de las cifras de penetración de internet. El último Censo Nacional de Población reporta que casi la mitad de los hogares tiene alguna cobertura de internet fija o móvil (43,4%) (25) y de uso de redes sociales; de los 48 millones de habitantes, más de 15 millones están registrados en Facebook, 78% de la población es usuaria de WhatsApp y cerca de 6 millones cuentan con Twitter (26,27). Sin embargo, la alfabetización digital en el país es muy baja, y el uso de las redes y el internet son predominantemente recreativos. Así, aunque un ciudadano colombiano pasa en promedio nueve horas al día en internet y cuatro horas en redes sociales (28), no es común que las personas entiendan bien cómo funciona el internet o para qué se usan sus datos. También, es usual que las personas no revisen en detalle las condiciones de uso y permisos de sus aplicaciones móviles o de las redes sociales que visitan constantemente.

En todo caso el rol del internet y lo digital en la vida humana solo parece aumentar, así como el tiempo dedicado a estos espacios y tecnologías. La pandemia de COVID-19 ha exacerbado esta tendencia al convertir lo virtual en el método más seguro para mantener la vida (y lo productivo) andando, mientras se profundizan medidas draconianas de distanciamiento físico. En el caso de Colombia las restricciones de movilidad y cuarentenas estrictas instauradas por los Decretos 457 de 2020, 531 de 2020, 536 de 2020 y 593 de 2020 llevaron a un aumento en el consumo de internet y a una ampliación de la cobertura en gran parte del país (29), lo que hizo evidentes



las inequidades estructurales en conectividad, disponibilidad y alfabetización tecnológica del país para algunas regiones.

Aún así, una mayor y mejor conectividad de las personas, así como la disponibilidad de teléfonos celulares y equipos con internet constituyen una gran oportunidad para el rastreo digital de contactos. Lo que se acompaña, también, de las preocupaciones por los posibles efectos no deseados de las intervenciones digitales en salud pública (16) en términos éticos, legales, técnicos e informáticos (30). Todo esto en un contexto donde las políticas (digitales) en salud pública han sido poco claras, verticales e impositivas hacia el público, en cuestiones como el acceso, la descarga, los permisos y los términos y condiciones de las estrategias para el rastreo de contactos. Usualmente, estas políticas se desarrollan en un escenario de gran tecnofilia y desconocimiento ingenieril, donde las personas (y a veces los mismos profesionales sanitarios y del gobierno) no son conscientes de las reglas algorítmicas o del uso y disposición de los datos, de cómo se recopilan, de quién más los podría usar, ni de qué se hace con estos al final del proceso de seguimiento médico.

La complejidad tecnológica del rastreo digital de contactos aumenta porque los datos para el seguimiento epidemiológico pueden conseguirse de diversas formas, de fuentes diferentes y a través de dispositivos distintos; por ejemplo, a través de los sistemas de geolocalización o Bluetooth (21) o de los registros de llamadas (31). Igualmente, gracias a la minería de datos producto de la vigilancia de redes sociales, se pueden conseguir datos de forma pasiva, simplemente ‘cosechando lo que los usuarios siembran’ sin que sean conscientes. Existe, a su vez, un sinnúmero de estrategias activas de recolección de datos en las que el usuario de telefonía celular ingresa a aplicaciones web móviles o descarga apps móviles nativas que con la mediación de API (*Application Programming Interfaces*) de Google y Apple, permiten, por ejemplo, la interacción entre dispositivos móviles en proximidades (17), dejando sus datos personales desprotegidos. Igualmente, el usuario puede diligenciar otros formatos digitales mediante el buscador de páginas web o *browser*, como las encuestas electrónicas para el reporte en los sistemas de vigilancia (32), desconociendo el protocolo de custodia de esta información. Esto demuestra que la transparencia en el proceso de consecución de los datos y la confianza depositada en la acción pública podrían minarse fácilmente con prácticas de cosechas de datos poco claras para los ciudadanos, yendo en contra de los ideales de la vigilancia en salud pública (2) en el marco de Estados de derechos. En esta diversidad de opciones para el rastreo yace tanto su potencial como los cuidados que amerita.

Este artículo espera mostrar que el rastreo digital de contactos desde la salud pública debe considerar, por lo menos, los asuntos de privacidad y de seguridad informática de los datos de las personas, así como prácticas transparentes y cuidadosas con las condiciones de obtención y uso subsecuente de la información. Ello se extiende a otros dominios de la vida social –más allá de lo sanitario– considerando los riesgos de la vigilancia ciudadana (en sentido político), la posible mercantilización de los datos, la violación de las libertades individuales y las preocupaciones sobre los límites del gobierno de la vida. Todo esto, a la luz del principio hipocrático por excelencia: ante todo no harás daño, que debe orientar el tipo de salud pública que se quiere hacer

y se puede hacer con la tecnología digital. Esto porque las políticas públicas de rastreo digital pueden elegir entre enfoques punitivos, vigilantes, coercitivos frente a las acciones individuales o, mejor, colaborativos, educadores, emancipadores para el cuidado de sí mismo y de los otros.

Para esto, se ilustra el caso del rastreo digital de contactos en Colombia, que en el mes de julio de 2020 ocupaba el quinto puesto en contagios por coronavirus en la región de las Américas (33), y en septiembre ya estaba en el quinto escalafón del mundo (34). Considerando que, desde marzo de 2020, Colombia desplegó una variedad de aplicaciones móviles para rastreo y vigilancia epidemiológica en lo nacional y lo local que pusieron el tema en la agenda pública, con su respectivo eco en las redes sociales por parte de la ciudadanía.

Así, se presenta primero una caracterización de aplicaciones móviles creadas en Colombia para el rastreo digital de contactos por la pandemia de COVID-19 entre marzo y septiembre de 2020 (incluido); seguido de un énfasis en la aplicación CoronApp respaldada por el gobierno nacional y con uso obligatorio para varias actividades de la vida cotidiana a esta fecha; terminando con un análisis de la discusión ciudadana sobre estas intervenciones en salud pública y su alcance.

## Métodos

Se realizó una etnografía digital en el sentido de la propuesta de Hine (35), entendida como una inmersión en la esfera virtual de las relaciones sociales para captar las minucias de la vida cotidiana de forma más franca y desinhibida y, en el caso de la pandemia por COVID-19, entendiendo el espacio de lo digital como gran resonador de las preocupaciones ciudadanas en medio del confinamiento físico. Esta etnografía habilita técnicas de captura de datos situadas en el flujo de la existencia cotidiana donde, en lugar de buscar activamente información y preguntar sobre lo que está pasando, se despliega un ejercicio de atención profunda a los datos producidos en redes sociales y medios de comunicación digital, dando lugar también a la interpretación y el cuestionamiento contextual de las interacciones en los usuarios de los espacios online (2015).

Entre marzo y septiembre de 2020 se rastrearon en la red social Twitter y en Google Colombia todas las publicaciones y tipos de contenidos (textos, imágenes, videos) que contenían información relacionada con las aplicaciones móviles de rastreo, con una técnica de observación no participante. Así mismo se visitaron las tiendas en línea de Android y iOS para identificar aplicaciones móviles para rastreo de contactos de COVID-19 en Colombia.

Si bien Facebook es la red social más usada en el país, los contenidos y lógicas algorítmicas de esta son diferentes a los buscados en este estudio, por lo que fue excluida de la selección. En ese sentido Twitter es un lugar virtual de debate sobre decisiones políticas y cuestiones sociales y Google es el medio de comunicación y búsqueda de información electrónico por excelencia en Colombia. Así, Twitter es frecuentada por más de seis millones de personas, y en esta se consolidan las cuentas institucionales de diferentes organizaciones del Estado, figuras sociales y





políticas, organizaciones no gubernamentales y otros grupos de interés que no están disponibles en otras redes, creando una dinámica discursiva de gran riqueza para la investigación social. Para el caso de Google Colombia se ejecutó una consulta los días 25 de julio y 17 de agosto de 2020 con la cadena de búsqueda: (“Aplicación” OR “APP” AND “coronavirus” OR “COVID”). Se parametrizaron los criterios de inclusión, así: “Fecha: último año”, “Páginas: en español”, “País: Colombia” y se obtuvieron 128 publicaciones sobre distintas aplicaciones digitales. De estos registros se excluyeron todos los resultados no relacionados con las aplicaciones para COVID-19 (N=20) y se eliminaron 40 publicaciones para países diferentes a Colombia. Al final se analizaron 68 publicaciones de Google sobre aplicaciones móviles para coronavirus en Colombia.

La cosecha en Twitter se realizó desde la cuenta personal de una de las investigadoras con base en el sistema de búsqueda automática de la plataforma. Allí se exploraron todas las publicaciones y contenidos trinados para el periodo comprendido entre 01 de marzo a 01 de septiembre de 2020 con la etiqueta de búsqueda “#Coronapp” y el filtro en idioma español. Al final se encontraron 59 publicaciones y de estas solo se excluyó una aplicación web sospechosa. Los 58 trinos restantes, con sus respectivos comentarios, fueron descargados como pantallazos en un archivo de Microsoft Word organizados por fecha y se leyeron cada uno en un ejercicio de pares entre las autoras.

La cosecha de las dos búsquedas se realizó de forma manual. Con los datos de identificación de los archivos captados diariamente se crearon dos bases en Microsoft Excel con el registro detallado de cada una de las fuentes: Google y Twitter. Para los datos de Google se visitó cada uno de los sitios web arrojados en la búsqueda, se realizó una lectura de los contenidos propuestos y se identificaron las aplicaciones para rastreo de COVID-19. Para estas se registraron la fecha de lanzamiento, el nombre de la aplicación, la población objetivo, la entidad creadora, el enlace de la publicación y el link de descarga de la misma.

En el caso de Twitter se registró para cada trino: el autor, la imagen del trino, la fecha del trino, el número de comentarios, número de re-tweets, número de ‘me gusta’ y un breve análisis del comentario frente a las aplicaciones de rastreo: crítico, a favor o neutro. Los comentarios de los trinos fueron captados junto con estos en una gran base. En algunos pocos casos, los comentarios fueron repetitivos y las investigadoras seleccionaron intencionalmente aquellos que presentaran los argumentos comunes con mayor claridad para el análisis posterior.

Para complementar la exploración digital de las aplicaciones, las investigadoras visitaron las tiendas en línea de iOS (AppStore) y Android (PlayStore), donde se registraron datos de la fecha de liberación, el número de descargas y el número de comentarios de todas las aplicaciones registradas con las palabras claves: “COVID” o “coronavirus” y la ubicación Colombia. Estos análisis son mostrados en otras publicaciones.

Todos los datos captados de Google, Twitter y las tiendas en línea, fueron codificados por las investigadoras de manera abierta en categorías emergentes utilizando el software para análisis

de datos cualitativos NVivo, con licencia de la Universidad de las investigadoras, y se presentan siguiendo un análisis de contenido de los principales hallazgos.

## Resultados

La pandemia de COVID-19 es el primer evento global que se combate digitalmente, lo que significa un nuevo universo de posibilidades para la salud pública, pero, también, retos sociales y ciudadanos sobre el gobierno de la salud y la vida que no deben pasarse por alto. En este contexto, las aplicaciones para el rastreo digital de los contagiados y sus contactos se han convertido en una de las principales estrategias de la caja de herramientas anti-pandémica, por lo que su análisis se convierte en un imperativo para el futuro del campo y la práctica salubrista.

En la búsqueda conducida en Google Colombia se encontraron referencias a 16 aplicaciones móviles para el rastreo de contactos de COVID-19, así como aplicativos web para el control de actividades laborales –el ingreso a oficinas–, sociales –como el ingreso a espacios comerciales– y de movilidad –el desplazamiento por ciertos lugares de las ciudades–. Estas tecnologías fueron Bogotá cuidadora/APP GABO, CaliValleCorona, CoronaApp, COVID-19 Boyacá, COVIDAPP, Cuidémonos, EsperanzApp, GeoVictoria, MeCuido App, Medellín me Cuida, Miscua, Registro COVID, Ruta de vida, Salud en orden, Sanare y StopCOVID. Ver detalles en la tabla 1. La mayoría de estas publicaciones fueron noticias (53%) o información oficial de los entes territoriales (28%).

**Tabla 1** Aplicaciones móviles disponibles en las tiendas en línea de PlayStore y AppStore para la vigilancia de casos de coronavirus. Colombia, septiembre de 2020

Nº	Nombre APP	Población objetivo	En Play-Store	Disponible en	Nº descargas	Nº comentarios	Entidad creadora	Fecha de creación o lanzamiento
1	CoronaAPP	Nacional	Sí	AppStore	10.000.000+	66.776	Instituto Nacional de Salud, Col.	Marzo 08, 2020
2	CoronaCare	Salud total	Sí	AppStore	5.000+	33	PaxeraHealth + Massachusetts General Hospital	Junio, 2020
3	Valle Corona	Valle del Cauca	Sí	NO	10.000+	148	Gobernación del Valle del Cauca	Mayo 06, 2020
4	COVID-19 Boyacá	Boyacá	Sí	NO	10.000+	124	Gobernación de Boyacá	Mayo 06, 2020
5	Yo me cuido Yo te cuido	Empresas	Sí	APKpure	1.000+	3	pruebalogistico	Mayo 12, 2020
6	GABO - Gobierno Abierto Bogotá APP	Bogotá	Sí	AppStore	100.000+	839	Alcaldía de Bogotá	Junio 01, 2020
7	Regreso Seguro Empresas	SURA	Sí	NO	5.000+	28	Suramericana	Julio 03, 2020
8	MeCuido Unal	UNAL	Sí	APKpure	500+	9	Universidad Nacional de Colombia	Mayo 02, 2020
9	Ruta de vida	Valle del Cauca	Sí	APKpure	5.000+	57	LiDARit INC	Abril 04, 2020
10	Salud en orden	Valledupar	Sí	APKpure	100+	2	Hanner Jose Coronel - Secretario de Salud de Valledupar	Marzo 26, 2020
11	Quidate	B/quilla	Sí	AppStore	10+	0	Alcaldía Distrital de Barranquilla	Abril 22, 2020

Fuente: tiendas en línea de PlayStore y AppStore.

En la lectura de los materiales de Google se identificó que algunas de estas tecnologías digitales no estaban relacionadas directamente con el rastreo de contactos, como el caso de COVIDAPP,





dirigida a la comunicación de pacientes seropositivos con sus médicos tratantes, o Medellín me Cuida con énfasis en las actividades de reactivación del comercio en la ciudad. En otras el alcance era específico para unos grupos poblacionales como Geovictoria, una aplicación chilena privada ofrecida en su momento al gobierno colombiano para el uso en los centros penitenciarios, o MeCuidoApp que luego se llamó MecuidoUNAL, dirigida a personal del Hospital Universitario Nacional. Otras aplicaciones tenían un énfasis territorial específico como App GABO para Bogotá, Sanare creada por la Universidad Autónoma de Manizales y cedida a la Administración Municipal, o Ruta de Vida, promovida por la gobernación del Valle del Cauca con un fuerte énfasis en el rastreo por geolocalización. También se identificó que la Procuraduría General de la Nación le solicitó a la Alcaldía de Cartagena evaluar la pertinencia de la App Cuidémonos, dada la existencia de otra aplicación de carácter nacional (CoronApp). Y junto con esta, a COVID-19 Boyacá y EsperanzApp del departamento de Risaralda, la Superintendencia de Industria y Comercio les requirió aclaraciones sobre la protección de los derechos de hábeas data de sus usuarios. Vale resaltar que a noviembre de 2020 algunas de estas aplicaciones habían tenido cambios en sus nombres, sus alcances o ya no se encontraban activas para su descarga en las tiendas en línea.

CoronApp, por su parte, era la aplicación promovida por el Gobierno nacional con el apoyo de diversos actores públicos y privados, la cual había logrado a noviembre de 2020 más de 10 millones de descargas y el mayor uso en el país. Según el Ministerio de Salud y Protección Social, su finalidad es que los ciudadanos tengan “información sobre el COVID-19, sus síntomas y medidas para prevenirlo”. Además, “es gratis y se puede obtener en las tiendas Android y en App Store” (36). Con estas características e intencionalidad, podría pensarse que su adopción ha sido un proceso exitoso, pero lejos está de ser una solución incuestionable.

Al intentar rastrear su origen se identificaron dos versiones posibles. Una, indicando que ésta fue creada en 2017 para determinar qué personas podrían ser potenciales focos o agentes infecciosos en las aglomeraciones de la visita del papa Francisco a Colombia y prevenir con ello posibles brotes de enfermedad (37). La otra, sobre cómo fue introducida por la firma encuestadora Guarumo, con afinidad política al gobierno de turno, y podría tener fines de seguimiento poblacional no solo epidemiológicos (38). Este asunto generó un revuelo en redes sociales y algunos usuarios expresaron su preocupación frente a la posibilidad de que se utilizaran estos datos para el ‘perfilamiento’ de los ciudadanos (Usuario Twitter 7) y para aprovecharse del miedo a la pandemia (Usuario Twitter 1). Uno de los comentarios más explosivos sobre la aplicación lo realizó el senador Gustavo Bolívar el 17 de junio de 2020 (68 comentarios, 924 *likes*, 680 *retweets*), presentándola como una especie de ‘trampa’ para quienes la instalaron, porque “cayeron” en una cierta preferencia política. Diversos usuarios respondieron sobre este trino con una queja en común: la instalación automática (no solicitada) de la aplicación en sus celulares cuando ellos descargaron otros programas no relacionados o actualizaron el teléfono (Usuarios Twitter 4, 5, 6), expresando que esta práctica era intrusiva. Asimismo, varios otros indicaron que cuando trataron de desinstalarla el equipo no se los permitía porque aparecía como aplicación de fábrica, por lo que solo podían bloquearla (Usuario Twitter 2, 3) (figura 1).

## INSTALACIÓN Y AUTO-INSTALACIÓN



**Figura 1** Pantallazos seleccionados en Twitter Colombia sobre los procesos de instalación y autoinstalación de CoronApp

Fuente: recortes de la etnografía digital en Twitter Colombia, junio 2020. El orden en que se muestran las imágenes no corresponde a una secuencia 'real' de cómo se produjeron o muestran en Twitter y se presentan acá para efectos interpretativos.

Algunos usuarios expresaron preocupaciones sobre el funcionamiento de las aplicaciones, sobre la obligación de registrarse con los datos personales, su lentitud, su poca usabilidad, sus problemas en la recolección de datos, el no funcionamiento *offline*, las continuas notificaciones y el exacerbado envío de propagandas. Encontrar estos problemas en las aplicaciones del gobierno tiene sentido porque la actualización y la respuesta a los usuarios demanda una gran disponibilidad humana y tecnológica, y el sector público no cuenta con la trayectoria ni la capacidad instalada para crear, sostener, mejorar o escalar con las mismas condiciones que sí podría hacerlo el sector comercial que confía en las plataformas digitales para su comercio electrónico. El problema aparece cuando el Estado utiliza el registro de estas aplicaciones para definir acciones de control o como requisito para algún trámite que afecta a la persona fuera del ámbito médico. Este ha sido el caso de las aplicaciones CoronApp o Bogotá me cuida.

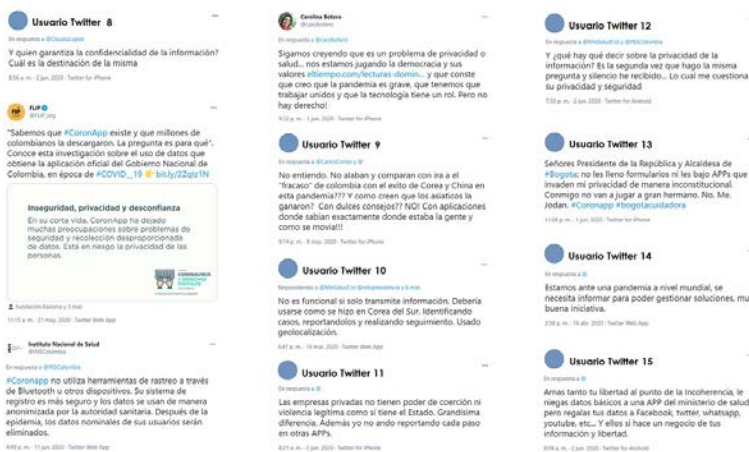
Otro asunto muy controversial sobre el uso de tecnologías para el rastreo de COVID-19 estuvo relacionado con sus implicaciones en términos de seguridad, privacidad (Usuario Twitter 9, 11, @FLIP\_org) y confidencialidad de los datos (Usuario Twitter 8).

Algunos usuarios de las redes solicitaron profundizar el uso de la información para el control de la enfermedad citando experiencias de otros países como Corea del Sur y China (Usuario Twitter 10, 13) y requiriendo el uso de la geolocalización para el seguimiento estrecho de los casos en el país. Al respecto, el Instituto Nacional de Salud en su cuenta de Twitter negó que la herramienta utilizara tecnologías de rastreo como GPS (Sistema de Posicionamiento Global, por sus siglas en inglés) y/o Bluetooth (39) o que fuera posible hacer identificación personal, dado que se basaban en datos anonimizados. Pero la solicitud de estos permisos por la App fue reportada en redes sociales, en las que se evidenció como una de las mayores preocupaciones ciudadanas (Usuario Twitter 9, @FLIP\_org).



También, varias personas solicitaron mayor cautela con el uso de esta información, la claridad sobre su finalidad y la relevancia de estas intervenciones para las discusiones democráticas y los valores ciudadanos (@carobotero, Usuario Twitter 11). Varios usuarios (Twitter 14 y 15) introdujeron la discusión sobre la diferencia entre proveer información personal como usuario a las redes sociales (en el sentido de empresas privadas), y el hecho de que el Estado mismo solicite los datos y los pueda usar para fines de coerción y/o violencia legítima (figura 2). En ese sentido, como bien lo indican desde la fundación Karisma (@carobotero), esta discusión no es solo sobre la privacidad o la salud, sino que “nos estamos jugando la democracia”.

### PRIVACIDAD DE LOS DATOS Y USO DE TECNOLOGÍAS DE RASTREO



**Figura 2** Pantallazos seleccionados en Twitter sobre privacidad, seguridad y uso de las tecnologías de rastreo de contactos para COVID-19 en Colombia

Fuente: recortes de la etnografía digital en Twitter Colombia, marzo a septiembre de 2020.

El orden en que se muestran las imágenes no corresponde a la secuencia en que se produjeron o mostraron en Twitter. Se presentan acá para efectos interpretativos.

Así como la funcionalidad de la aplicación y la confidencialidad fueron motivos de preocupación, el surgimiento de prácticas autoritarias mediadas por lo digital y el rol de la policía en estos nuevos escenarios fueron expresados en varias ocasiones. @Carobotero de la fundación Karisma puso en discusión el hecho de que la aplicación aparece como voluntaria, pero gobierna aspectos de la vida cotidiana, en particular asuntos como las restricciones de movilidad impuestas en las ciudades, en las empresas y hasta para el tráfico aéreo, que la hacen mandatoria para diversos momentos y poblaciones. En el mismo sentido, en las redes se discutieron las posibles limitaciones que la ‘necesidad’ de la app impone a varios grupos por la falta de acceso a las condiciones tecnológicas esperadas. Tal es el caso de defensores de derechos humanos y periodistas, las personas en las regiones con problemas de conectividad (@CarlosCortes, @partidodelaucol) o, inclusive, de los grupos étnicos (@Karisma 14 de marzo). La mención de estas brechas y prácticas diferenciales por los usuarios de las redes y no por las autoridades (@Karisma 14 de marzo y 31 de agosto), así como la falta de una estrategia epidemiológica

clara mediada por estas aplicaciones de cara a la ciudadanía (usuario twitter 18), permiten el surgimiento de dudas sobre su efectividad, legitimidad (Usuario Twitter 16) y utilidad social (Usuario Twitter 19).

De la misma manera, es evidente que la tensión entre el Estado ‘cuidador’ y el Estado ‘vigilante’, apoyado en las tecnologías digitales en salud, debe ser puesta en la arena pública (Usuario Twitter 17) para discutir cómo llevar a cabo la vigilancia epidemiológica y, en un sentido más amplio, la salud pública mediada por datos. Esto debe conducir hacia prácticas que garanticen la salud a la vez que protejan la información de las personas como derechos ciudadanos (Usuario Twitter 16).

Otro asunto que despertó la inquietud de los tuiteros fue el uso final de los datos. No solo la vigilancia por parte del Estado parece una opción alarmante, sino el hecho de que la información sensible (recordemos que toda información sanitaria lo es) sea vendida a otros actores, en un acto de mercantilización de la confianza de los usuarios-pacientes por sus gobiernos. Ver figura 3.

### OTRAS PROBLEMÁTICAS



**Figura 3** Pantallazos seleccionados en Twitter sobre privacidad, seguridad y uso de las tecnologías de rastreo de contactos para COVID-19 en Colombia

Fuente: recortes de la etnografía digital en Twitter Colombia, marzo a septiembre de 2020.

Muchos otros asuntos que se discutieron en las redes, Google y en las aplicaciones no se presentan acá, pero vale rescatar tres más por considerarlos relevantes para concluir esta aproximación. Primero, se destacó la ausencia de medidas y protocolos claros para la prevención de discriminación de población reportada positiva en la aplicación, esto ante las crecientes muestras de intolerancia en el público general para los pacientes COVID-19. Segundo, se hizo un llamado a considerar el costo de inversión para la implementación y mantenimiento de estas herramientas sin las garantías de su efectividad, en momentos de crisis fiscales y necesidades



económicas profundas. Finalmente, el hecho de que las aplicaciones para el rastreo se basen en la idea de que la información y la comunicación son los principales activos para combatir la enfermedad, sin aclarar sus condiciones de uso, hace que la gente sienta desconfianza frente a la aplicación como estrategia en salud pública. Esto termina deslegitimando estas intervenciones y su posible impacto poblacional.

## Discusión y conclusiones

El trabajo sintetiza el estado de la discusión en la red social Twitter sobre la creación, implementación y uso de aplicaciones y estrategias digitales para el rastreo de contactos por COVID-19 en Colombia, en momentos de gran tensión social del año pandémico 2020. La elección de Twitter (40) se debió a su carácter eminentemente discursivo. Twitter está orientado a la presentación y debate de ideas y argumentos para entender las diversas manifestaciones sociales frente a las aplicaciones en estudio (41). Aunque no se realizó una comparación ni diferenciación con los datos y discusiones en Facebook, la red más usada en el país, los elementos presentados son valiosos para posicionar el tema en la discusión del campo y en la arena política y social. El trabajo llevó a cabo un análisis de las discusiones sobre el uso de la tecnología en la salud pública y sus consideraciones en una lectura más amplia de la relación Estado-Ciudadano.

Es innegable que, mientras los profesionales de la salud pública de todo el mundo trabajan incansablemente para responder a la pandemia de COVID-19, toda estrategia que fortalezca las técnicas tradicionales de rastreo de contactos merece ser considerada para abordar una crisis de alcance y velocidad sin precedentes (13). En ese sentido, las tecnologías digitales en rápido desarrollo parecen servir para la contención y vigilancia de la evolución de la pandemia, prometiendo ser parte esencial de la caja de herramientas para la prevención y control de futuros brotes infecciosos (18). Esto significa, claro está, una variación importante en la forma de realizar la práctica epidemiológica y el control poblacional.

Si bien diversos países han creado tecnologías digitales para apoyar el control de la infección, estas no pueden ignorar la creciente preocupación social y las quejas ciudadanas (21,42), además de reconocer que no son la ‘bala mágica’ de la salud pública (16,21). Estas consideraciones parecen encontrar un término común: pocas garantías de confidencialidad en el manejo de los datos, posible invasión a la privacidad a través de la vigilancia continua o con fines no sanitarios, riesgo de mercantilización de la información, preocupaciones sobre el poder del Estado, de sus instituciones y los derechos ciudadanos digitales, así como poca claridad en la política epidemiológica sobre el uso de la información. (17,21). Otras preocupaciones son propias de las condiciones del lugar, como las relacionadas con el perfilamiento político en el caso de la historia colombiana.

Las recomendaciones posibles para abordar esta discusión podrían resumirse, inicialmente, en tres categorías: técnica, sanitaria y sociopolítica. En un sentido más técnico (17) se sugiere considerar, por lo menos:



Quién(es) está(n) detrás del proceso de producción de las tecnologías para así abordar los intereses, las plataformas y arquitecturas que soportan, así como las reglas de juego en las que se producen, recolectan y utilizarán los datos posteriormente. En síntesis, cuán transparentes y claros son los creadores con los usuarios.

Cuáles son las condiciones técnicas de uso, qué permisos solicita, qué datos recolecta, su obligatoriedad, en qué tiendas en línea está disponible, qué protocolos cumple, cuáles son los estándares de privacidad y seguridad. Cómo reduce la recolección de datos a aquellos exclusivamente necesarios para la finalidad sanitaria declarada, protegiendo al usuario.

Cuál es el modelo epidemiológico y la estrategia de salud pública que las soporta. Allí vale preguntarse por los criterios epidemiológicos y las modelaciones en los que se sustentan los algoritmos de identificación de contacto, así como por las estrategias de rastreo y contención de la enfermedad.

Cómo han sido sus indicadores de uso, cuántas veces y dónde se ha descargado, cuáles son los comentarios de los usuarios sobre su funcionalidad, cuáles sobre la usabilidad, cómo funciona en la práctica y, en general, qué nivel de penetración ha alcanzado.

Cuáles son los procesos de disposición, archivo y borrado de los datos una vez sus usos sanitarios han sido cumplidos.

Cuáles son las políticas sociales y técnicas que protegen a las y los ciudadanos de cualquier abuso, además de garantizar la confianza y la participación social en los escenarios de decisión y uso de la información.

Varios de estos asuntos han sido considerados en los informes publicados por la Organización no gubernamental Karisma, que analizó varias aplicaciones acá referenciadas y encontró que "... estas apps tienen permisos muy intrusivos para la privacidad, como la localización aproximada y fina (GPS). Por lo tanto, la aplicación tiene la posibilidad de localizarnos en tiempo real" (43 párrafo 9). Asimismo, señala que el proceso de abogacía ciudadana no ha devenido en un mejoramiento de estas características en las aplicaciones, incluyendo CoronApp. Esto evidencia la fragilidad de los procesos deliberativos democráticos y la falta de canales para comprender el rol de las intervenciones digitales y su impacto en las vidas de las y los ciudadanos.

En relación con lo socio sanitario se han discutido muchos asuntos. Uno de estos tiene que ver con las consideraciones éticas de este tipo de intervenciones digitales (21). Recordemos que en el sector salud los usuarios son habitualmente pacientes y sus datos se protegen con consideraciones éticas especiales dada la condición de vulnerabilidad y la asimetría entre estos y los profesionales sanitarios. Así, cuando los datos de salud superan la esfera hospitalaria y pasan al Estado, este debe actuar con las mismas lógicas protectoras con las cuales se





procede en la clínica, orientadas por el juramento hipocrático: procurar la beneficencia de la acción-intervención individual y social, evitar cualquier daño posible, respetar la autonomía de las personas y sus libertades, garantizar la solidaridad, justicia y equidad en las acciones e intervenciones y salvaguardar la privacidad y confidencialidad de las personas, así como procurar la legitimidad pública y la transparencia (44). A estas lógicas de protección médica deben añadirse aquellas propias de los tratados sobre hábeas data y protección de datos personales que rijan en el territorio.

El tema digital (señales, bits y datos) en el sector salud, es uno de los más relevantes en el presente y de los más retadores de cara al futuro. Esto se debe a que el sector utiliza las herramientas digitales como uno de sus principales insumos para la asistencia en salud y la protección de la vida de las personas, asumiendo a las personas y sus procesos de atención como fuentes de datos esenciales, esto es, las personas como datos. Sin embargo, en los procesos de digitalización del sector se ha dejado por fuera la idea contraria de que, cuando se utiliza la información sobre los pacientes y sobre sus procesos de atención, los datos con lo que se trabaja terminan alterando las decisiones y la vida de las personas. En ese sentido, de una manera relacional e imbricada, no hay intervención digital que no esté mediada por un cuerpo humano. Así, cuando se registra un caso de COVID-19 en una aplicación, cuando se le niega a alguien la posibilidad de viajar, cuando se le permite a alguien retornar a su trabajo o cuando se identifica un contacto, en todos esos procesos *datificados* hay personas, sujetos de derechos plenos aún en lo digital. Por ello las decisiones clínicas y sociales mediadas por lo virtual, deben pasar a la esfera de la discusión social amplia y consciente, superando una tecnofilia imperante en el sector y una suerte de ingenuidad sobre los futuros digitales posibles.

En ese sentido, reconociendo los límites del rastreo de contactos físico en situaciones de gran tumulto social y vertiginosa expansión del virus, vale la pena preguntarse por las ventajas de este y sobre cómo la tecnología puede potenciarlo y no desplazarlo (17). De este modo, no se pierde de vista la potencia del seguimiento físico, de la confianza y persuasión humana, así como de la capacidad de adaptación de las personas a las características y necesidades de sus pares. Estos elementos hacen que el proceso de seguimiento y cuidado de la salud (no solo de rastreo) sea más efectivo (8). Por lo que la pregunta es, ¿cuál es el rol de la tecnología en la sociedad (y por ende en una práctica salubrista) que proteja la salud de las personas al tiempo que respeta sus derechos y contribuya a vidas dignas y seguras?

Frente al último asunto puesto en la agenda social por la discusión de las redes, las implicaciones sociopolíticas de las aplicaciones digitales de rastreo de casos y las demás intervenciones tecnológicas en salud requieren poner sobre la mesa diversas cuestiones y hacerlo de manera responsable. Es imperativo que las autoridades gubernamentales garanticen en sus políticas públicas medidas de protección y rutas de acciones claras para salvaguardar la privacidad de los usuarios y la protección de sus datos. Esto implica especialmente la protección de sus derechos ciudadanos mediados por la esfera digital. La discusión se debe concentrar en los valores ciudadanos que rigen el pacto social dominante y los futuros posibles sobre los que se construirán las relaciones de la sociedad tecnológica. Esta cuestión lleva varias décadas

en la arena sociopolítica, puesta allí por los estudios sociotécnicos como el de Winner (45) que revelan el rol de las tecnologías en la definición de la vida, en la profundización de inequidades y en la producción de modos de habitar el mundo físico. Las características de los algoritmos, las condiciones técnicas de seguridad y privacidad de las aplicaciones y de los aplicativos en web, los acuerdos tácitos o no sobre el uso de los datos y su finalidad, pueden contribuir a soluciones digitales asertivas, sostenibles, aceptadas y útiles. No obstante, también pueden minar la legitimidad del accionar en salud pública y la relación de las personas con las instituciones y el Estado. El reto está en construir y sostener soluciones adecuadas y respetuosas en lo ético y legal, en cuanto a seguridad y privacidad, que superen los estados de emergencia y excepción en épocas de pandemia, y se conviertan en estrategias efectivas para soportar las acciones sanitarias poblacionales en una base continua.

Como lo expresa Roche (21), los sistemas de rastreo de contactos poseen riesgos inherentes, por lo que la labor de las intervenciones mediadas por lo digital, es considerar la connivencia y surgimiento de nuevos desafíos que amenacen o pongan en riesgo a las personas, así como conciliar acciones para proteger la salud y la vida, fin mismo de cualquier intervención en salud pública, aún en lo digital.

## **Consideraciones éticas**

El trabajo respetó las consideraciones éticas para la investigación en los seres humanos recomendado en las pautas internacionales del Comité de investigación de la OMS (CIOMS), la legislación sobre Hábeas Data en Colombia (Resolución 1266 de 2008), garantizando que todos los datos que se recopilaban de las redes sociales han sido anonimizados y solo se usan para esta finalidad académica. Dada la naturaleza digital de la metodología el estudio se consideró sin riesgo según la declaración del artículo 11 de la Resolución 008430 de 1993 que reglamenta la investigación en salud con seres humanos.

## **Contribución de las autoras**

Este trabajo surge en el seno de un proyecto de grado de la Maestría en salud pública en la Pontificia Universidad Javeriana de Bogotá, Colombia.

## **Financiación**

Las autoras no recibieron ningún dinero por la realización de este artículo. Sandra Agudelo es profesora universitaria y su salario cubrió la realización de estas actividades de investigación. Clara Núñez dedicó el tiempo propio de su proceso de formación como magister en salud pública. Se agradece a la Pontificia Universidad Javeriana por el tiempo.

## **Conflictos de intereses**

Las autoras manifiestan no tener ningún conflicto de intereses.



## Referencias

1. Organización Mundial de la Salud - OMS; 2020. <https://www.who.int/es/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020>
2. Berman E, Fowler L, Roberts J. COVID-19 Surveillance. 2020;1-71. <https://doi.org/10.2139/ssrn.3666300>
3. García-Iglesias J, Martín-Pereira M, Fagundo-Rivera J, Gómez-Salgado J. Herramientas de vigilancia digital para el rastreo de contactos de personas contagiadas de SARS-COV-2. *Rev Esp Salud Pública*. 2020;23(94):e202006067. <http://rabida.uhu.es/dspace/handle/10272/18455>
4. Rosen G. A history of public health New York: MD Publications, Inc.; 1958.
5. Semmelweis I. Etiología, concepto y profilaxis de la fiebre puerperal [1861] (extraídos). *Medicina Social*. 2008;3:21-29. <https://www.medicinasocial.info/index.php/medicinasocial/article/view/188>
6. Spooner J. History of Surgical Face Masks: The myths, the masks, and the men and women behind them. *AORN J*. 1967;5(1):76-80. [https://doi.org/10.1016/S0001-2092\(08\)71359-0](https://doi.org/10.1016/S0001-2092(08)71359-0)
7. Snowden F. *Epidemics and Society: From the Black Death* New Haven and London: Yale University Press; 2019. DOI: 10.1007/s12115-020-00517-z
8. Mooney G. "A Menace to the Public Health" — Contact Tracing. *The New England Journal of Medicine*. 2020;383:1806-1808. <https://doi.org/10.1056/NEJMp2021887>
9. Welch G. El rastreo de contactos de casos de COVID-19 será la investigación sanitaria más compleja de la historia; 2020. <https://www.nationalgeographic.es/ciencia/2020/05/rastreo-de-contactos-casos-covid-19-investigacion-sanitaria-mas-compleja>
10. Vallès X, Carnicer-Pont D, Casabona J. Estudios de contactos para infecciones de transmisión sexual. ¿Una actividad descuidada? *Gaceta Sanitaria*. 2011;25(3):224-236. <https://doi.org/10.1016/j.gaceta.2010.12.003>
11. Klausner J, Wolf W, Fischer-Ponce L, Zolt I, Katz M. Tracing a Syphilis Outbreak Through Cyberspace. *JAMA*. 2000;284(4):447-449. <https://doi.org/10.1001/jama.284.4.447>
12. University of Cambridge; 2020. <https://www.cl.cam.ac.uk/research/srg/netos/projects/archive/fluphone2/>
13. Anglemeyer A, Moore T, Parker L, Chambers T, Grady A, Chiu K, et al. Digital contact tracing technologies in epidemics: A rapid review. *Cochrane Database of Systematic Reviews*. 2020;8(CD013699):1-44. <https://doi.org/10.1002/14651858.CD013699>
14. Eysenbach G. Infodemiology and Infoveillance: Framework for an Emerging Set of Public Health Informatics Methods to Analyze Search, Communication and Publication Behavior on the Internet. *J Med Internet Res*. 2009;11(1). <https://doi.org/10.2196/jmir.1157>
15. Mavragani A. Infodemiology and Infoveillance: Scoping Review. *J Med Internet Res*. 2020;22(4):e16206. <https://doi.org/10.2196/16206>

16. Agudelo-Londoño SM. Reflexión sobre la evaluación de impacto en eSalud. «No todo lo que brilla es oro». Trilogía Ciencia Tecnología Sociedad. 2020;12(22):103-126. <https://doi.org/10.22430/21457778.1262>
17. Owusu P. Digital technology applications for contact tracing: the new promise for COVID-19 and beyond? Global Health Research and Policy. 2020;5(36):1-3. <https://doi.org/10.1186/s41256-020-00164-1>
18. Ivers L, Weitzner D. Can digital contact tracing make up for lost time? The Lancet Public Health. 2020;5(8):e417-8. [https://doi.org/10.1016/S2468-2667\(20\)30160-2](https://doi.org/10.1016/S2468-2667(20)30160-2)
19. MIT Technology Review; 2020. <https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/>
20. López-Alberto C, Soto-Ramón C. Filosofía de lo imprevisible, reflexiones para la pandemia. México DF: Editores y Viceversa; 2020.
21. Roche S. Smile, you're being traced! Some thoughts about the ethical issues of digital contact tracing applications. Journal of Location Based Services. 2020; 14(1):71-91. <https://doi.org/10.1080/17489725.2020.1811409>
22. Ybañez S, Bonanno F. Medidas internas aplicadas por el gobierno chino ante la emergencia del COVID-19. In Busso A. Relaciones internacionales en tiempo de pandemia (pp. 92-97). Rosario: Edición para Centro de Investigaciones en Política y Economía Internacional (CIPEI); 2020.
23. Velásquez A. Fundación Karisma; 2020. <https://web.karisma.org.co/aplicaciones-de-rastreo-digital-de-contactos-para-que-zapatos-si-no-hay-casa/>
24. OCDE - Organización para la Cooperación y el Desarrollo Económicos; 2020. <https://www.oecd.org/gov/Colombia-Scan-Final-Spanish.pdf>
25. Departamento Administrativo Nacional de Estadística - DANE; 2019. <https://www.dane.gov.co/files/censo2018/informacion-tecnica/cnpv-2018-presentacion-3ra-entrega.pdf>
26. Ministerio de Tecnologías de la Información y las Comunicaciones; 2020. <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Sabia-Ud-que/2713:Colombia-es-uno-de-los-paises-con-mas-usuarios-en-redes-sociales-en-la-region>
27. Deloitte; 2020. [https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Brochure\\_ConsumoMovil\\_CO\\_LATAM\\_2020.pdf](https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology-media-telecommunications/Brochure_ConsumoMovil_CO_LATAM_2020.pdf)
28. Neira-Marciales L. La República; 2020. <https://www.larepublica.co/empresas/un-colombiano-pasa-nueve-horas-al-dia-en-internet-y-casi-cuatro-en-redes-sociales-2975617>
29. Leal-Acosta A. La República; 2020. <https://www.larepublica.co/empresas/en-abril-el-uso-de-internet-en-colombia-aumento-115-frente-a-marzo-de-este-ano-3010517>
30. Kahn J (ed.) Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance Baltimore: Johns Hopkins University Press; 2020.



31. Nisar S, Zuhaib M, Ulasyar A, Tariq M. A Privacy Preserved and Cost Efficient Control Scheme for Coronavirus Outbreak Using Call Data Record and Contact Tracing. *IEEE Consumer Electronics Magazine*. 2020;10(2):104-110. <https://doi.org/10.1109/MCE.2020.3038023>
32. Avaro D, Berchi M, Stropparo P. Entre barbijos: reflexiones acerca de la libertad en la pandemia. Argentina: Fundación Apolo; 2020.
33. Romero V. *El Tiempo*; 2020. <https://www.eltiempo.com/mundo/mas-regiones/coronavirus-como-esta-colombia-con-respecto-al-resto-del-mundo-524350>
34. Moreno M. *El Tiempo*; 2020. <https://www.eltiempo.com/salud/colombia-supera-las-25-000-muertes-por-coronavirus-539988>
35. Hine C. *Ethnography for the Internet* New York: Routledge; 2015.
36. @MinSaludCol. Twitter web app; 2020. <https://twitter.com/minsaludcol/status/1240419680520724482?lang=es>
37. INS Colombia. YouTube; 2020. <https://www.youtube.com/watch?v=oqf2ldtPGTc>
38. @GustavoBolívar. Twitter.; 2020. <https://twitter.com/gustavobolivar/status/1273290621730664452?lang=es>
39. @INSColombia. Twitter Web App.; 2020. <https://twitter.com/INSColombia/status/1271197856863596549>
40. Rosgaby-Medina K. Branch.; 2020. <https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2019-y-2020/>
41. Ovadia S. Exploring the Potential of Twitter as a Research Tool. *Behavioral & Social Sciences Librarian*. 2009; 28(4):202-205. <https://doi.org/10.1080/01639260903280888>
42. TIME. <https://time.com/>; 2020. <https://time.com/5898559/covid-19-contact-tracing-apps-privacy/>
43. Castellanos A, Labarthe S.; 2020. <https://web.karisma.org.co/permisos-de-las-apps-de-covid-cuando-bajara-esta-curva/>
44. Aguilera B. Asignación ética de recursos sanitarios escasos en el contexto de crisis por COVID-19. *Medwave*. 2020;20(5):e7935. <https://doi.org/10.5867/medwave.2020.05.7935>
45. Winner L. Do artifacts have politics? *Daedalus*. 1980; 109(1):121-136. <http://www.jstor.org/stable/20024652>