¿Son las tecnologías digitales el mejor recurso para controlar el contagio del Covid-19? El reto de la protección de los datos personales.

Lina Paola Velásquez Veloza[1]

Resumen.

La humanidad se ha enfrentado a pandemias durante toda la historia y ha estado inmersa la búsqueda de soluciones alternativas para contrarrestar los contagios y combatirlas a través de la ciencia. La diferencia de este episodio con las demás pandemias es que contamos con tecnología avanzada y soluciones más rápidas. De las herramientas nuevas a las que acudió la humanidad en este siglo ha sido el uso de las tecnologías digitales, que permiten el acceso a la información de cada ciudadano, con el propósito de rastrear e identificar el contagio en situaciones específicas como en lugares y contactos con personas que hayan sido contagiadas o que están en riesgo de contagiarse. Sin embargo, la desesperación por mantener el control de contagios de Covid-19 permitió un fácil acceso a la privacidad e intimidad de las personas sin su consentimiento, dejando de lado la protección de los derechos fundamentales en materia de datos personales y la normatividad nacional e internacional que desarrolla las obligaciones de los Estados con dicha protección.

Palabras clave: Datos personales, tecnologías digitales, pandemia, contagios, políticas públicas, acceso, protección de datos personales, derechos fundamentales, privacidad, intimidad.

Introducción.

¿Son las tecnologías digitales el mejor recurso para controlar el contagio del Covid-19?

Las tecnologías digitales han permitido el fácil acceso a nuestra vida privada y a los datos que permiten nuestra identificación, un claro ejemplo es el caso controversial que se presentó a inicios de este año, en el que Facebook compartió la información de los usuarios con la aplicación WhatsApp, sin que los usuarios tuvieran la oportunidad de escoger si rechazar y no aceptar los términos y condiciones establecidos por la misma *app*[2]. Un acto muy común en el mundo y que en Colombia no es la excepción.

El uso de dichas tecnologías, han sido una de las principales herramientas a las que han acudido los gobiernos para mantener el control de contagios de Covid-19 sobre los ciudadanos. Un claro ejemplo son los casos de Corea del Sur, donde realizan rastreos digitales a través de las cámaras de vigilancia, datos ubicados en los teléfonos inteligentes de pacientes con coronavirus y así publicar los datos de quienes salieron de sus casas[3].

---

[1] Abogada egresada de la Universidad La Gran Colombia. Investigadora y semillerista, fue Auxiliar Judicial Ad Honorem en la Corte Constitucional Colombiana (2020)

[2] BBC News Mundo. "WhatsApp es bastante intrusivo y Facebook es un buitre de los datos": Carissa Véliz, experta en privacidad y protección de información" por: Boris Miranda https://www.bbc.com/mundo/noticias-55683865

[3] Ibidem.

En Italia, las autoridades realizaron rastreos con los teléfonos inteligentes, permitiendo ubicar las distancias típicas que recorrieron los ciudadanos todos los días. Por último, en Israel se utilizó un caché de datos de ubicación de teléfonos móviles para identificar a los ciudadanos que pudieron estar expuestos al virus[4]. Acciones gubernamentales que han sido el foco principal de inconformismo al no ofrecer una materialización real en las políticas públicas que permitieran garantizar los derechos de los ciudadanos en materia de la privacidad.

Los datos personales son informaciones asociadas a: (…) *una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos*[5].

De allí que parte la importancia de proteger los datos como base principal de la privacidad, intimidad de los ciudadanos, la dignidad humana, al acceso a la información y la autodeterminación informática, la libertad, la libertad de expresión y la libertad informativa, al buen nombre y entre otros derechos.

La investigación estará encaminada a comprobar si el uso de las tecnologías digitales por parte del Estado afecta directamente a la población, al tenerlas como herramientas para mitigar el contagio del Covid-19. Se observó durante todo el año de la pandemia que la decisión de los Estados y Gobiernos de implementar el control del contagio a través del uso de estas herramientas digitales alteró la privacidad de los ciudadanos, es por ello, que las organizaciones y movimientos que promueven la protección de los derechos digitales denunciaron la falta de límites y la inseguridad que esto generaba.

El uso de estas plataformas les permitió a las entidades estatales realizar el seguimiento de cada acción y movimiento que realizaba cada uno de los ciudadanos sin que hubiere paso al respeto por la privacidad. Hubo quejas alrededor de la aplicación de estas políticas públicas al no tener en cuenta la afectación que implicaba el que el Estado esté vigilando los movimientos de la población.

De lo anterior, se presenta una posible hipótesis sobre la grave afectación a la privacidad de los ciudadanos al aplicar este tipo de plataformas sin un adecuado estudio previo en las políticas públicas por parte del Estado.

De esta forma como objetivo general se visualiza el "Analizar la aplicación de las políticas públicas que se implementó por parte de los distritos en relación con el control del contagio del Covid-19 en Colombia".

I. Normatividad nacional e internacional en relación con el derecho a la privacidad e intimidad.

[4] The New York Times. "As Coronavirus Surveillance Escalates, Personal Privacy Plummets" https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

[5] Superintendencia de Industria y Comercio en relación con la Protección de Datos Personales https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Es así, como a nivel internacional, se tiene que la Declaración Universal de los Derechos Humanos, protege este derecho a través del artículo 12 el cual dispone la prohibición de ser objeto de *"injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación"*[6]. El Pacto de los Derechos Civiles y Políticos establece el derecho de ser protegido o protegida por la ley *"contra esas injerencias o esos ataques"*[7] y la regulación a la libertad de expresión, *"el derecho a la libertad de buscar, recibir y difundir informaciones e ideas de toda índole"* así como la protección de *"(...) a) Asegurar el respeto a los derechos o a la reputación de los demás; y b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas"*[8].

De otro lado, a nivel internacional, se encuentra la Convención de las Naciones Unidas contra la Corrupción, en la cual se dispone la obligación de los Estados de aplicar el principio de transparencia sobre las actividades, como los procedimientos o reglamentaciones aplicadas por las entidades públicas[9], que permita garantizar el acceso a la información a la ciudadanía.

En Colombia, nuestra Constitución prevé la protección de datos en el artículo 15, que desarrolla el derecho de todas las personas a su intimidad personal y familiar, buen nombre y el derecho a *"reconocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"*[10], prohibiendo el tratamiento de datos personales en los casos que exceptúa la ley.

A partir de la expedición de la Constitución Política, se emitieron leyes[11] que regulan la protección de los datos personales, la implementación de una entidad encargada de vigilar y sancionar la violación a estos derechos y el desarrollo de la efectividad en los procesos de quejas de los ciudadanos ante una invasión en su intimidad, permitiendo desenvolver las obligaciones del país sobre dicho acceso.

II. El uso de las tecnologías digitales en el Distrito ante la emergencia sanitaria por COVID-19.

Durante la pandemia en Bogotá, desde que llegó el primer caso de contagio de Covid-19, el distrito optó por tomar medidas que permitieran el control de contagios, a través del rastreo e identificación de los casos de personas contagiadas de coronavirus para mejorar el gestionamiento ante la crisis sanitaria. Es por ello, que la Alcaldía emitió el Decreto 131 de 2020[12], que dispuso la creación de dos aplicaciones, GABO APP y la plataforma digital Bogotá Cuidadora. La Alcaldía indicó que la información que se recolectan estas dos últimas aplicaciones, sirve para *"hacer*

---

[6] La Declaración Universal de los Derechos Humanos disponible en: https://www.un.org/es/about-us/universal-declaration-of-human-rights

[7] Congreso de la República, Ley Nº 74 de 1968, (23 de marzo de 1976). Recuperado (10/08/2021) de la URL: https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx. Pacto Internacional de Derechos Civiles y Políticos (Ratificado por Colombia: 29 de octubre de 1969) Art. 17

[8] Ídem. Art. 19

[9] Convención de las Naciones Unidas contra la Corrupción Disponible en: https://www.unodc.org/colombia/es/convencionONU.html

[10] Constitución Política de Colombia. (1991) Recuperado (08/08/2021) de la URL: https://www.suin-juriscol.gov.co/viewDocument.asp?id=1687988

[11] Leyes 1266 de 2008, la Ley 1581 de 2013 y el Decreto 1377 de 2013

[12] Por el cual se imparten lineamientos para dar continuidad a la ejecución de la medida de aislamiento obligatorio en Bogotá D.C. y se toman otras determinaciones. Disponible en: https://bogota.gov.co/mi-ciudad/seguridad/cuarentena/conoce-el-decreto-131-de-2020-sobre-el-aislamiento-parcial-en-bogota

vigilancia epidemiológica y gestión de movilidad segura"[13] y que se trata de *"una herramienta de cuidado colectivo. Entre más personas se registren, tendremos más información para orientar acciones focalizadas de prevención del contagio*"[14].

El control que se llevaría a cabo con estos medios digitales, corresponde a la recolección de información que permitiría prevenir las aglomeraciones de personas en puntos específicos de la ciudad, el ajuste de ofertas de servicios distritales como el transporte público, entre otras medidas sanitarias. Normatividad que fue controvertida al entenderse la obligatoriedad sobre la instalación de estas aplicaciones para transitar dentro de la capital, limitando los derechos fundamentales de los ciudadanos como la libertad de locomoción y el fácil acceso que tuvieron las aplicaciones para acceder a los datos personales de los ciudadanos[15].

En cuanto a la acreditación personal del ciudadano a través de esta aplicación, bastará con realizar dicha acreditación una sola vez, indicando la ruta que usará el ciudadano y los horarios preponderantes. Tiene otras formas de apoyo sobre el control de contagio a través de los índices, *"Necesito apoyo",* que permite atender al ciudadano a través de apoyo económico del distrito; *"Reportar estado de salud"* para prestar atención rápida y efectiva ante síntomas agudos de coronavirus; *"COVID-19 a mi alrededor"* accede a mapas y datos para facilitar la información sobre el número de contagios en la localidad y por edad; y por último, *"Ofrezco ayuda"* para aquellos ciudadanos que quieran ser parte de la red de apoyo en el distrito.

Sin embargo, la Superintendencia de Industria y Comercio (SIC), autoridad encargada de proteger los datos personales, realizó las investigaciones pertinentes, donde se encontró que las aplicaciones permitían la exposición de seis carpetas con datos privados que facilitaba el acceso sin autorización, tales como actas de grado y diplomas de personas naturales, cédulas de ciudadanía, actas de exhumación, entre otros[16].

De esta manera, a través de la Resolución 45002 la SIC ordenó la implementación de medidas apropiadas y efectivas sobre las plataformas digitales y su fortalecimiento en materia de seguridad, acceso y uso limitado, circulación restringida y confidencialidad de los datos sensibles[17]. Ante las discusiones presentadas por los ciudadanos y diferentes organizaciones no gubernamentales[18], la Alcaldía emitió un nuevo Decreto, con aclaración sobre la obligatoriedad de la descarga de la aplicación, convirtiéndola en una opción voluntaria por parte del ciudadano[19].

Aún con lo anterior, el laboratorio de seguridad digital y privacidad de la Fundación Karisma *(K+Lab)*, realizó el análisis de las plataformas digitales del distrito anteriormente

---

[13] "Así funciona Bogotá Cuidadora, la 'app' del Gobierno Abierto de Bogotá (GABO)" artículo de la página oficial del distrito disponible en: https://bogota.gov.co/asi-vamos/gabo/gabo-app-y-bogota-cuidadora-que-es-preguntas-y-respuestas

[14] Ídem.

[15] Publimetro. "¿Bogotá Cuidadora o controladora? La polémica por la aplicación de la Alcaldía" por Juan Manuel Reyes Fajardo. Disponible en: https://www.publimetro.co/co/noticias/2020/06/02/bogota-cuidadora-controladora-la-polemica-la-aplicacion-la-alcaldia.html

[16] SIC imparte instrucciones para que GABO APP sea más segura. Artículo de Ámbito Jurídico en: https://www.ambitojuridico.com/noticias/tecnologia/constitucional-y-derechos-humanos/sic-imparte-instrucciones-para-que-gabo-app

[17] Resolución disponible en: https://www.sic.gov.co/slider/la-superintendencia-de-industria-y-comercio-en-su-calidad-de-autoridad-nacional-de-protecci%C3%B3n-de-datos-se-permite-informar-lo-siguiente-1

[18] Es el caso de la Fundación Karisma, ONG que trabaja en la promoción de los derechos humanos en el mundo digital. Página web disponible en: https://web.karisma.org.co/

[19] Decreto 134 de 2020. https://bogota.gov.co/mi-ciudad/salud/cuarentena/conoce-el-decreto-134-de-2020-en-bogota

mencionadas, en las que Stéphane Labarthe[20] indica que los datos no quedan a disposición directamente de la Alcaldía sino que la aplicación GABO se transmite a una IP que corresponde a un servidor web de Microsoft ubicado en Estados Unidos. De allí parte la importancia de su regularización, si se tiene en cuenta que las personas que no son ciudadanas estadounidenses, no gozan de la protección de datos personales.

Por otro lado, también presentó como una de las preocupaciones más relevantes como el fácil acceso a la cámara y a la localización del dispositivo determinando que se corre un riesgo en materia de privacidad por no contar con los permisos legales y que aún, si los tuviera, en relación con las diligencias distritales, *"crea un conflicto con la privacidad de la ciudadanía cuando se incluye "Bogotá Cuidadora" como otra funcionalidad de la aplicación y ésta gestiona datos tan sensibles"*[21].

Adicional a ello, la investigación mostró que la plataforma Bogotá Cuidadora genera un rastreo en el dispositivo de los usuarios por parte de Microsoft para fines publicitarios al instalar varios cookies que están directamente asociados a dominios de esa multinacional[22]. De todo lo anterior, el caso de Bogotá no fue el único caso en encontrarse este tipo de fallas en materia de protección, la Fundación Karisma también encontró que las aplicaciones como CoronApp Colombia, Medellín Me Cuida y CaliValle Corona presentaron las mismas afectaciones a los derechos de privacidad de los ciudadanos del sector[23].

Muchas de las críticas que giran en torno a estas plataformas digitales en desarrollo debido a la pandemia se basan en ¿qué tan útiles pueden llegar a ser estas herramientas? y ¿acosta de qué? Estos cuestionamientos no solo se han desarrollado en el marco distrital o nacional en Colombia. El MIT Technology Review sugirió, sobre el caso de Islandia, que "no deberíamos poner demasiadas esperanzas en una solución digital" debido a que este país, a pesar de tener la tasa de penetración más alta de todos los rastreadores de contactos del mundo, no se ofreció mayor apoyo sobre el control del Covid-19[24].

En Islandia se lanzó una aplicación de rastreo respaldada por el gobierno llamado Racking C-19, la cual era voluntaria y con dependencia a permisos para la publicación de datos, analiza los datos del GPS de los usuarios para mapear dónde han estado para ayudar al equipo de rastreo de contactos de Islandia. Los datos de ubicación quedan guardados en los dispositivos de los usuarios y si el equipo de seguimiento de contactos necesita su ayuda, debe enviar una solicitud de información y si los usuarios están de acuerdo, sus datos se almacenan durante 14 días en la base de datos del equipo de rastreo[25].

Esta plataforma, tuvo la tasa de descarga más alta del mundo[26], pero no por ello demostraba una efectividad en el control de los contagios y aglomeraciones en el marco de la pandemia,

[20] "Rastreo digital en Bogotá" estudio publicado en la página web de la Fundación Karisma disponible en: https://web.karisma.org.co/rastreo-digital-en-bogota/
[21] Stéphane Labarthe en la investigación mencionada en la línea anterior.
[22] ibídem.
[23] "Bogotá Cuidadora levantó ampolla", artículo escrito por Carolina Botero. Disponible en: https://web.karisma.org.co/bogota-cuidadora-levanto-ampolla/
[24] How Effective Are Contact Tracing Apps? Disponible en: https://slate.com/technology/2020/05/contact-tracing-apps-less-effective-iceland.html
[25] ibídem
[26] ibídem.

conclusión que ya se había desarrollado en la Fundación Karisma en relación con CoronApp Colombia[27].

III. Estudios y recomendaciones sobre la aplicabilidad del uso de las tecnologías digitales en tiempos de pandemia.

Por todo lo anterior, se han realizado diversos estudios y análisis alrededor de estas problemáticas digitales. Está el estudio realizado por un grupo de médicos e investigadores en el sector de la salud publicado en la Revista de Bioética y Derecho[28] en el que para darle una debida protección al uso de los datos personales descompone la Ley 1581 de 2012 unificándola con las recomendaciones éticas de la OMS de la siguiente forma:

Tabla No. 1. *Principios (Ley 1581 de 2012) Recomendaciones éticas OMS*

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

Tomado de Scielo. Revista de Bioética y Derecho. Versión On-line ISSN 1886-5887. 2020.

Tabla No. 2. *Derechos (Ley 1581 de 2012) Recomendaciones éticas OMS*

[27] CoronApp: muchos datos, ¿pocos beneficios? Disponible en: https://web.karisma.org.co/coronapp-muchos-datos-pocos-beneficios/

[28] Revista de Bioética y Derecho. Artículo. "El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia". Ana Gómez-Córdoba, Sinay Arévalo-Leal, Diana Bernal-Camargo, Daniela Rosero de los Ríos. no.50 Barcelona 2020. Disponible en: https://scielo.isciii.es/scielo.php?pid=S1886-58872020000300017&script=sci_arttext&tlng=pt#B31

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

Tomado de SciELO. Revista de Bioética y Derecho. Versión On-line ISSN 1886-5887. 2020

Investigación que demuestra que a pesar de haber un desarrollo normativo amplio, que obedece a las recomendaciones de la OMS estudiadas por el equipo médico en mención, aún existen fallas en la aplicación de políticas públicas. De lo anterior, se ha concluido que es un tema de debate no solamente en Colombia sino que también se ha presentado en el continente latino. El Observatorio de tecnologías de vigilancia y pandemia, desarrolló un estudio sobre el uso de estas plataformas y aplicaciones en Latinoamérica con ocasión a la pandemia[29], para que los gobiernos puedan aplicar adecuados proyectos en temas de políticas públicas que tengan como fin el tratamiento de los datos personales a través de las tecnologías.

La primera recomendación que realizan los expertos es que el despliegue tecnológico desde el sector público debe ir acompañado de medidas estrictas de transparencia, participación y rendición de cuentas[30]. Es importante asumir el rol sobre la debida aplicación de tecnologías en el sector social si se tiene en cuenta que nuestras vidas ya giran en torno a las herramientas digitales, por lo que es relevante la reglamentación a través de políticas públicas reales que garanticen nuestros derechos fundamentales más allá del marco de la pandemia.

La segunda necesidad es romper con las barreras sociales de los sectores menos favorecidos en relación con el acceso a las tecnologías. El informe indica que "*(...) en nuestra región aún existe un número no reducido de personas que, por edad, condición económica, origen étnico o incluso por factores de género carecen de la posibilidad de acceder y controlar un dispositivo de carácter personal"*[31].

[29] Informe Observatorio Covid-19 del Consorcio Al Sur: Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia. Junio, 2021. Pág. 65. Disponible en: https://web.karisma.org.co/tecnologias-digitales-para-la-pandemia-al-tablero-varias-soluciones-desplegadas-en-paises-de-la-region/

[30] ibídem. Pág. 65.

[31] Ibídem. Pág. 66.

Por lo que se sugiere, la aplicación de diseños digitales que permita el uso de estas aplicaciones sobre un mismo dispositivo, con la debida protección de datos.

Por otro lado, como tercer punto, el observatorio indica la importancia del acompañamiento de las políticas públicas en el sector público y privado. En el informe se concluyó que el tratamiento de los datos personales no corresponde exclusivamente al sector público sino que también a las empresas privadas[32]. Por ende, la implementación del despliegue de estas tecnologías deberá garantizar otros derechos como la privacidad, acceso a la información, no discriminación, derecho a reunión, movilidad, derecho al trabajo entre otros.

En cuarto lugar, el desarrollo de la definición de los proyectos tecnológicos con información debidamente estructurada. El Observatorio indica que se corroboró que al tratarse de la aplicación de estas políticas públicas hay poca definición en la información ofrecida a los usuarios sobre el tratamiento de sus datos personales. Por lo que ofrecen ideas sobre la aplicación de medidas de seguridad como:

> *(…) el cifrado (en almacenamiento y tránsito de la información), arquitecturas de datos descentralizadas y límites temporales al almacenamiento de datos, son aún elementos limitadamente incorporados o ausentes en la mayor parte de las iniciativas identificadas, todos elementos relevantes para una gobernanza que por diseño privilegie la adecuada protección de los datos personales recogidos y la implementación de límites cuando se trate de contextos políticos.*

Por último, la transparencia como principio que permite entender, controlar y generar vínculos de confianza en asuntos de tecnologías como estrategia contra el Covid-19.

Otro complemento a estas sugerencias dadas por parte del Observatorio, es la de la Comisión de la Unión Europea que determinó varias directrices sobre el uso de las aplicaciones de uso voluntario en el marco de la pandemia[33], dentro los cuales están (i) información precisa para los usuarios sobre la pandemia de coronavirus; (ii) cuestionarios de autodiagnóstico y orientación individualizada (función de comprobación de síntomas); (iii) alertas dirigidas a personas que han estado cerca de una persona infectada para que se hagan una prueba o se aíslen (función de localización de los contactos y de alerta); y (iv) un foro de comunicación entre médicos y pacientes en aislamiento voluntario en el que se ofrece asesoramiento adicional en materia de diagnóstico y tratamiento (telemedicina).

Lo anterior, con las condiciones normativas del uso adecuado del tratamiento de los datos personales de los ciudadanos: (i) la responsabilidad de las autoridades sanitarias nacionales; (ii) los usuarios conservan el pleno control de sus datos personales; (iii) uso limitado de datos personales; (iv) límites estrictos al almacenamiento de datos, (v) seguridad de los datos; (vi) garantía de la exactitud de los datos tratados y (vii) participación de las autoridades nacionales de protección de datos[34].

---

[32] Ibídem. Pág. 67.
[33] Coronavirus: Directrices para garantizar unas normas de plena protección de los datos en las aplicaciones para luchar contra la pandemia. Comisión de la Unión Europea. 16 de abril de 2020. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_20_669
[34] Ibídem.

IV. Conclusiones.

1. A pesar de existir estudios y recomendaciones internacionales, los gobiernos y en este caso las alcaldías, no desarrollaron un plan de gobierno adecuado a los estándares normativos que protegen los datos personales.
2. Se marca un precedente en el país sobre el mal uso de las tecnologías en temas de salubridad alarmantes, como fue en el caso del covid-19, con la creación de normatividades distritales que afectaron directamente los derechos fundamentales de los ciudadanos, por lo que las alcaldías pueden aprender de estos errores aplicando el mejoramiento en las aplicaciones y herramientas tecnológicas, en relación a los datos personales e información sensible.
3. En Colombia, contamos con normas que sí regulan la protección de los datos personales, con una entidad encargada de vigilar y sancionar las decisiones administrativas de los diferentes municipios y gobernaciones del país, que contraríen la normatividad y la Constitución Política de Colombia.
4. El uso de las tecnologías digitales no es la solución absoluta al control del Covid-19 en el mundo y especialmente en Latinoamérica, por la dificultad para acceder a dichas tecnologías, como es en el caso de Colombia. Razón por la cual, también se debe buscar políticas públicas que apoyen y faciliten a las comunidades el acceso a la información y a los dispositivos digitales.
5. Debe haber un estudio de fondo sobre el desarrollo de las aplicaciones para no afectar de manera tan abrupta la intimidad y la privacidad de los ciudadanos, regulando estas formas de acceder a los datos personales cuando se trate de plataformas digitales que tienen control en otros países.

Referencias bibliográficas.

"Buscamos saber en qué se está movilizando la gente en Bogotá": Alcaldía. (2020). Semana.

Botero, C. (8 de junio de 2020). Fundación Karisma. Obtenido de “Bogotá Cuidadora levantó ampolla”: https://web.karisma.org.co/bogota-cuidadora-levanto-ampolla/

Constitución Política de Colombia [Const. P.]. (1991). Colombia. Obtenido el 18 de agosto de 2021. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Convención de las Naciones Unidas contra la Corrupción. (s.f.).

Coronavirus: Directrices para garantizar unas normas de plena protección de los datos en las aplicaciones para luchar contra la pandemia. Comisión de la Unión Europea. (16 de abril de 2020).

Decreto 131, mayo 31, 2020. Alcaldía Mayor de Bogotá. Obtenido el 18 de agosto de 2021. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=106394

Decreto 134, junio 2, 2020. Alcaldía Mayor de Bogotá. Obtenido el 18 de agosto de 2021. https://bogota.gov.co/mi-ciudad/salud/cuarentena/conoce-el-decreto-134-de-2020-en-bogota

Decreto Ley 1377, junio 27, 2013. Presidencia De La República. Obtenido el 25 de febrero de 2021.

http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

Fajardo, J. M. (s.f.). "¿Bogotá Cuidadora o controladora? La polémica por la aplicación de la Alcaldía". Publimetro.

Gómez, A., Arévalo, S., Bernal, D., y Rosero, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Bioética y Derecho.*

Hadavas, C. (2020). How Effective Are Contact Tracing Apps? Slate.

Índice coronavirus y derechos digitales Colombia. (21 de mayo de 2020). Fundación Karisma. Obtenido de CoronApp: muchos datos, ¿pocos beneficios?: https://web.karisma.org.co/coronapp-muchos-datos-pocos-beneficios/

La Declaración Universal de los Derechos Humanos. (s.f.).

Labarthe, S. (2020 de junio de 2020). Fundación Karisma. Obtenido de https://web.karisma.org.co/rastreo-digital-en-bogota/

Ley 1266/2008, diciembre 31, 2008. Diario Oficial [D.O.]: 47219. (Colombia). Obtenido el 18 de agosto de 2021. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Ley 1581/2012, octubre 18, 2012. Diario Oficial [D.O.]: 48587. (Colombia). Obtenido el 18 de agosto de 2021. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Ley 74/1968, diciembre 30, 1974. Diario Oficial [D.O.]: 32682. (Colombia). Obtenido el 18 de agosto de 2021. https://www.icbf.gov.co/cargues/avance/docs/ley_0074_1968.htm

Miranda, B. (29 de enero de 2021). *WhatsApp es bastante intrusivo y Facebook es un buitre de los datos": Carissa Véliz, experta en privacidad y protección de información*. BBC News Mundo.

Observatorio Covid-19 del Consorcio Al Sur. (2021). Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia.

Pacto Internacional de Derechos Civiles y Políticos. (s.f.).

Página oficial del Distrito de Bogotá. (s.f.). Así funciona Bogotá Cuidadora, la 'app' del Gobierno Abierto de Bogotá (GABO).

Resolución 45002. (5 de agosto de 2020).

Sang-Hun, N. S. (23 de marzo de 2020). "As Coronavirus Surveillance Escalates, Personal Privacy Plummets" . The New York Times.

SIC imparte instrucciones para que GABO APP sea más segura. (11 de agosto de 2020). Ámbito Jurídico.

Superintendencia de Industria y Comercio en relación con la Protección de Datos Personales. (s.f.). Obtenido de https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales