LA DELGADA Y MÓVIL FRONTERA DE LAS *CORONA-APPS* EN AMÉRICA LATINA

Carolina Aguerre
19 de mayo de 2020

El 11 de marzo de 2020 la Organización Mundial de la Salud (OMS) declaró el estado de pandemia mundial por la expansión de la COVID-19 a más de 100 países. Cuatro días después, el grupo de relatores y expertos/as independientes del Consejo de Derechos Humanos de la Organización de Naciones Unidas (ONU) lanzó un comunicado alertando sobre las consecuencias para la observancia de los derechos humanos ante las diversas medidas que se vislumbraban, aunque ese comunicado no las especificaba. Tales amenazas se transformaron en una potencial realidad con la implementación de las llamadas *corona-apps* (entre otros neologismos surgidos en tiempos recientes), que en el caso de América Latina tomaron rápidamente vuelo.

Este artículo examina la evolución de las aplicaciones vinculadas a la pandemia ocasionada por la COVID-19 en el contexto regional de América Latina, y la discusión en torno a sus objetivos, su modelo de gobernanza y su inserción, diálogo y conflicto con los marcos institucionales y normativos vigentes, incluyendo los derechos humanos.

Antecedentes de las aplicaciones y su vínculo con la vigilancia

Durante la última década, las aplicaciones de rastreo, ubicación y monitoreo han proliferado en redes de datos móviles e inalámbricas, y a través de informes automáticos ejecutados por aplicaciones en teléfonos inteligentes que están equipados con chips del Sistema de Posicionamiento Global (GPS) (Hutchins, 2007). Es de conocimiento público que múltiples emprendimientos han aprovechado estas tecnologías basadas en la ubicación para fines comerciales, obteniendo acceso a una gran cantidad de datos en el proceso, incluyendo datos personales confidenciales[1].

Varios países de todo el mundo están desarrollando aplicaciones de seguimiento de contactos. Por lo general,

[1] El proyecto "PhoneFlu" desarrollado por investigadores de la Universidad de Cambridge, que coincidió con el brote de la gripe porcina, incursionó en estas técnicas con fines similares. Véase: https://www.cam.ac.uk/research/news/fluphone-disease-tracking-by-app.

usan datos de ubicación satelital o Bluetooth para registrar quién ha estado cerca de una persona. Esta información se puede usar para notificar a los usuarios si alguien que conocen se enferma con COVID-19 y declara su estado en la aplicación.

Si bien la mayor parte de la discusión reciente asociada con la vigilancia por parte del sector privado ha venido de la mano de conceptos como "capitalismo de datos" (Zuboff, 2019), vinculado al modelo de negocios de las grandes plataformas de internet, en el contexto de la pandemia emergen otros actores del sector privado que son parte integral del ecosistema de la conectividad, como las empresas de telecomunicaciones. El poder de vigilancia de estas empresas no ha escapado a la atención de diversas organizaciones vinculadas con la defensa de los derechos humanos, como Ranking Digital Rights, que desde sus orígenes ha incorporado el análisis de estos actores, en tanto su capacidad de monitoreo y vigilancia puede resultar aún más invasiva para la privacidad de la ciudadanía que la de muchas empresas que operan sobre la capa de contenidos (Ranking Digital Rights, 2019).

Es fundamental tener en cuenta que en América Latina el acceso a internet llega a casi el 70% de sus habitantes (Internet World Stats, 2019). Este acceso se logra mediante telefonía móvil en todos los casos donde hay al menos una conexión por persona (casi 450 millones de ciudadanos/as de la región están conectados mediante estos dispositivos) y, en los hogares más ricos, también mediante banda ancha fija y ordenadores. En Argentina, por ejemplo, el 60% de los hogares posee una computadora, mientras que el 84% posee al menos un dispositivo celular (INDEC, 2020). Sin embargo, en Centroamérica el promedio de conectividad a internet móvil es menor al 40% de la población. Esto pone de manifiesto que, si bien ha habido un avance en la penetración de las tecnologías de información y comunicación, esta no necesariamente permite aún el despliegue de políticas públicas de manera generalizada, que varían en cada contexto nacional y subnacional.

Dada la ubicuidad de los dispositivos celulares conectados a las redes móviles, estas tecnologías presentan oportunidades y ventajas concretas para el desarrollo de sistemas de información relevante para la ciudadanía en el contexto de la COVID-19.

El mayor riesgo de las aplicaciones digitales que están en proceso de implementación, o en sus primeras semanas de uso, deriva de que están explícitamente diseñadas para el rastreo de contactos. En términos generales, su funcionamiento se basa en el siguiente principio: el proceso de identificación se genera mediante la construcción de un contacto, que se registra con el número de teléfono

móvil y una identificación del usuario, anónima y aleatoria. La lista de contactos incluye un registro de los usuarios que han entrado en contacto cercano con un caso confirmado, a los que se les notifica los próximos pasos, como el autoaislamiento. Finalmente, el seguimiento implica una comunicación frecuente con los contactos para monitorear la aparición de cualquier síntoma y probar en consecuencia su confirmación.

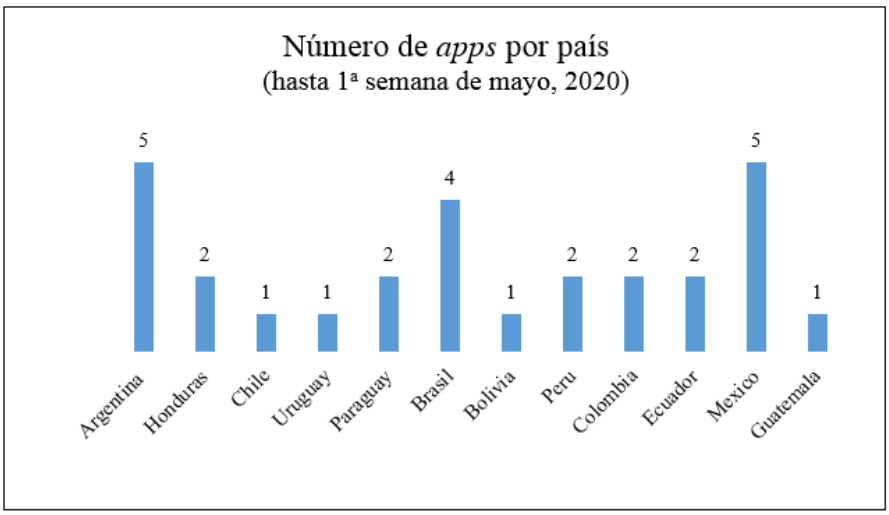
TraceTogether es la aplicación desarrollada en Singapur para atender la pandemia mediante un mecanismo de rastreo de contactos. Ha sido un caso analizado y retomado en distintos contextos en Asia, Europa y América Latina, con variaciones a partir de la adecuación a cada contexto, y teniendo en cuenta las lecciones aprendidas de su implementación, que no representó precisamente un factor de éxito para la contención de la pandemia en ese país (Financial Times, 2020).

TraceTogether utiliza la tecnología Bluetooth para detectar si los usuarios, que han incorporado la aplicación voluntariamente, se han ubicado a menos de nueve metros uno del otro, en lugar de recopilar datos de ubicación directamente de los operadores móviles. Esta y otras aplicaciones de rastreo de contactos generalmente almacenan datos entre 14 y 21 días de interacción de los participantes para ayudar a controlar la propagación de la enfermedad. El seguimiento generalmente lo realizan las agencias gubernamentales.

Aplicaciones en América Latina

El primer país de América Latina en desarrollar una *corona-app* fue Bolivia, el 15 de marzo, seguido de Colombia, el 16 de marzo, y luego Uruguay, que lanzó una aplicación el 20 de marzo. Desde entonces el aluvión de instrumentos no ha cesado de engrosar una lista cada vez más extensa, aun cuando presenten variaciones en su alcance, funcionalidad, modelo de gobernanza de datos y, por ende,

GRÁFICO 1



distintas amenazas en relación a los marcos institucionales y legales, y a los derechos humanos. Estos temas serán abordados en este apartado.

El Gráfico 1 refleja la evolución de las *corona-apps* en la región de acuerdo a un relevamiento propio realizado entre fines de abril y comienzos de mayo de 2020. El escenario es móvil y dinámico: a él se suman, semana a semana, no solo nuevas aplicaciones en distintos contextos nacionales, sino en distintas regiones, provincias y estados que desarrollan sus propios instrumentos.

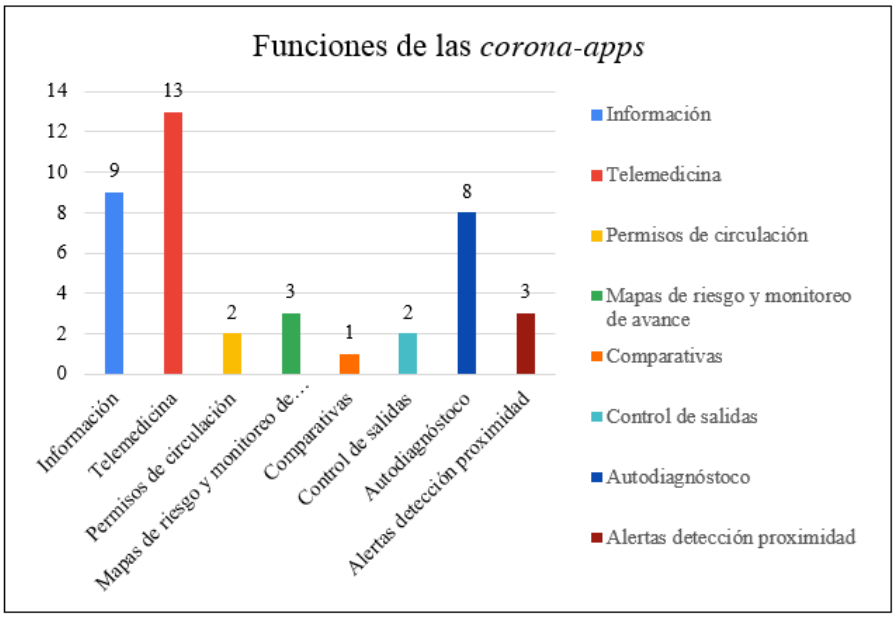
Varios países, sobre todo los que tienen una organización política federal, como Argentina, Brasil y México, desarrollaron más de una aplicación en distintos estados. También en Colombia, Paraguay, Perú, Honduras y Ecuador se han desplegado varias iniciativas correspondientes a distintas ciudades/regiones, así como aplicaciones diferenciadas para cumplir con varios objetivos. En muchos casos, esta proliferación también obedece a la fragmentación de los sistemas de salud.

El relevamiento de las funciones de las distintas aplicaciones constituye un desafío por su variabilidad en cortos períodos temporales, y por la capacidad de integrar nuevas funcionalidades. Por ejemplo, la aplicación de Uruguay —CoronavirusUY— creada por la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC), con el apoyo técnico de una empresa del país, empezó siendo una aplicación de localización de los puntos donde se habían registrado infecciones, e incorporó luego funcionalidades de consultas médicas a distancia e información general sobre la pandemia y las medidas del país. Más recientemente, ha anunciado su interés en la implementación del desarrollo conjunto de Apple y Google, con el fin de integrarlo. La aplicación CuidAR, en Argentina, ha tenido una evolución similar: a medida que ha avanzado la pandemia y el gobierno nacional ha tomado medidas, ha avanzado en su misión original, incluyendo cambios en su arquitectura técnica.

En el Gráfico 2 se detallan las principales funciones de las distintas aplicaciones, obtenidas a partir del relevamiento de sus descripciones en los sitios web oficiales y tiendas para su descarga.

Las principales funciones de las 28 aplicaciones relevadas hasta el momento de elaborar este análisis, muestran que la principal misión es la de brindar servicios de telemedicina, incluyendo el reporte de síntomas (disponible en 13 aplicaciones). Le sigue la función de suministrar información a los ciudadanos y, luego, la de autodiagnóstico. Las dos funcionalidades más controvertidas en términos de vigilancia son las de alerta por proximidad y la de control de salida.

GRÁFICO 2



El gran problema que suscitan estas funciones es que se encuentran publicadas y se corresponden con servicios e instrumentos a disposición de los ciudadanos. Sin embargo, se desconoce el uso de estos datos para confeccionar otro tipo de análisis que pueda interferir con la privacidad e intimidad de las personas.

Así es como la transparencia y la rendición de cuentas emergen como uno de los principales focos del debate sobre el uso de estas aplicaciones. Aun cuando declaren que solo se utilizan para algunos fines, el debate público de las últimas semanas en la región se ha centrado en los avances sobre su misión original, que se están produciendo sin una clara divulgación de sus políticas de almacenamiento, procesamiento y uso de los datos, al contrario de lo que establece la política de minimización de datos del Reglamento General para la Protección de Datos (RGPD) de la Unión Europea. Por ejemplo, CoronApp, de Colombia, publica dentro de sus funcionalidades en Play Store que: "Esta aplicación es una de las fuentes de datos para la toma de decisiones del Estado". Por ello, la sociedad civil ha demandado que el gobierno brinde mayores precisiones sobre los usos de los datos que apunta al rastreo digital de contactos por medio de Bluetooth (Velásquez, 2020). La cantidad de errores del desarrollo original de la aplicación está llevando al gobierno a implementar la tecnología conjunta de rastreo digital de contactos de Apple y Google, ya mencionada.

En América Latina todavía hay seis países que no poseen una ley de protección de datos personales. Sin embargo, estos han desarrollado sus propias *corona-apps*. Aun respetando los principios fundamentales para su

desarrollo, esta ausencia tiene el potencial de vulnerar la privacidad de la ciudadanía. Para mitigar estas debilidades normativas e institucionales, algunas aplicaciones se están basando por ejemplo en tecnología *blockchain*, como es el caso de la aplicación CIVITAS en Honduras. Es relevante anotar que Brasil no tiene aún implementada su ley: aprobada en 2018, la Ley General de Protección de Datos Personales iba a entrar en vigor en 2020, pero, debido a la pandemia, ha sido prorrogada a 2021.

El papel del Estado como promotor de estas iniciativas ocupa un rol fundamental en el mapa de *corona-apps* de la región. De las 28 iniciativas relevadas, casi la mitad se han originado por iniciativa gubernamental, seis de ellas pertenecen a empresas, dos poseen un origen mixto y, en ellas, la colaboración con las bases de datos del Ministerio de Salud resulta clave para su funcionamiento, como en el caso de la aplicación CoTrack, de la provincia de Mendoza en Argentina. Por último, hay media docena de aplicaciones que están activas, pero en las que no se especifica la organización que respalda su desarrollo. El panorama es todavía incierto en términos de evolución y consolidación de estas aplicaciones.

La colaboración público-privada es un ingrediente fundamental de estas aplicaciones. Si bien en la mayoría de los casos se ha encontrado una participación del Estado en la activación de las aplicaciones, prácticamente todas las iniciativas han desarrollado alianzas con empresas para su diseño e implementación.

Utilizando los cuatro principios rectores para el desarrollo de aplicaciones que ha promulgado la Unión Europea —voluntariedad, consentimiento, resguardo de la identidad y política de eliminación de los datos—, a continuación se examinan estos puntos, contrastándolos con el análisis de las aplicaciones que han surgido en la región.

Las políticas de eliminación de datos son específicas únicamente en tres de las *corona-apps* relevadas. En cuanto a los resguardos de identidad, únicamente seis tienen políticas que *por default* anonimizan o no toman datos personales. En el caso de CoronavirusUY, el usuario puede solicitar el resguardo de su identidad vía email; en la veintena de casos restantes no se aplica ninguna política en tal sentido, o no se hace explícita. Un caso innovador es el de la aplicación COVID-19 CDMX que, si bien toma datos sensibles, como la georreferencia, tiene un botón visible que permite “borrar información y almacenamiento de datos”. Si bien muchas aplicaciones mencionan en sus términos y condiciones que se puede solicitar la eliminación de datos, esta es la única que incorpora tal derecho en su interfaz.

En materia de almacenamiento, la mayoría de las aplicaciones usa servidores instalados en Estados Unidos. En el caso de la aplicación de Uruguay, los datos se almacenan en servidores de la AGESIC y, en el caso de CuidAR, la aplicación del gobierno nacional se gestiona con la infraestructura de la Empresa Argentina de Soluciones Satelitales (ARSAT). También hay casos, como Monitora Covid-19 (Brasil) o Alerta Guate (Guatemala), donde los datos se alojan en servidores de empresas privadas nacionales.

En lo que respecta a la voluntariedad, únicamente dos aplicaciones eran de uso preceptivo al momento de la publicación de este análisis: CuidAR en Argentina, para quienes provienen del exterior, contrajeron la enfermedad o tienen permiso de circulación para trabajar; y COVID-19 PY, en Paraguay. Las restantes aplicaciones se manejaban bajo el principio de la voluntariedad.

Más allá de la normativa europea, la voluntariedad es uno de los principios para el desarrollo de políticas basadas en estas aplicaciones. Sin embargo, de acuerdo con distintas aproximaciones, en un escenario de mínimos para ser efectivas es necesario contar con al menos el 40% de la población de un lugar determinado (como se aconseja en el caso de la aplicación en Australia), o del 60% como se recomienda en Reino Unido. De hecho, este ha sido uno de los factores por el cual TraceTogether de Singapur, que optó por el principio de voluntariedad, no tuvo éxito en la contención de la pandemia, ya que fue adoptada por menos del 20% de la población entre marzo y abril.

El consentimiento es el último principio del RGPD y, desde este marco, debe ser otorgado libremente, y debe ser específico, informado y sin ambigüedades. El incumplimiento de cualquiera de estos cuatro criterios invalida el consentimiento y, por ende, el procesamiento basado en este principio. En virtud de la información analizada, se constata que pocas aplicaciones de la región cumplirían con los principios que articula el RGPD.

Por último, se aborda el papel de las empresas de telecomunicaciones, mencionadas al inicio, en la implementación de las *corona-apps*. Hay algunos casos como el de México, donde la Agencia Digital de Innovación Pública (ADIP), solicitó acceso a las antenas satelitales para monitorear el correcto cumplimiento de la cuarentena para personas positivas con el virus. En Ecuador, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) desarrolló una plataforma para que los gobiernos seccionales pudieran monitorear aglomeraciones y hacer seguimiento de personas infectadas. Esta plataforma también cruza datos con la aplicación SaludEC para identificar en sus mapas las manza-

nas de las ciudades donde se encuentran los contagios. En Medellín, Colombia, también se han alcanzado acuerdos entre el Estado y las empresas de telecomunicaciones para detectar a posibles portadores del virus. En Brasil hay casos, como el de Rio, en los que la compañía TIM monitorea desplazamientos en la ciudad de forma anonimizada.

Entre la eficacia y la vigilancia permanente. Algunas consecuencias y reflexiones finales

Resulta innegable que la pandemia ocasionada por la COVID-19 genera vulnerabilidades sociales, económicas, políticas y sistémicas a nivel internacional, y que es imprescindible buscar todos los instrumentos posibles para desactivar su propagación y evitar sus externalidades negativas sobre tantas esferas. Las tecnologías de información y comunicación sustentadas en la inteligencia artificial, los grandes datos (*big data*), las redes basadas en protocolos de internet o los dispositivos cada vez más "inteligentes", han propiciado herramientas para tratar los múltiples desafíos que se presentan. Estas no han sido únicamente un salvoconducto para los Estados. La ciudadanía se ha refugiado en las oportunidades que ofrecen para realizar y suplir actividades que están vedadas en contextos de confinamiento.

Como en el pasado, la utopía en torno a las tecnologías resurge con fuerza. Y este resurgir no solo se produce desde un punto de vista instrumental, sino también teleológico, como en el camino para la solución de múltiples asuntos, entre ellos, la proliferación del virus. Este artículo ha intentado mostrar cómo el recorrido de las incipientes *corona-apps* de la región todavía presenta vaivenes, incertidumbres y dilemas, que reflejan problemas que no pudieron resolverse antes de la pandemia, y pone de manifiesto que el uso de la tecnología, en sí misma, no puede resolver problemas de fondo. El escenario se presenta aún más complejo en la medida que, sin marcos adecuados, se dificultan las garantías que establecen los mecanismos de rendición de cuentas de las autoridades sobre los datos recabados. Este desafío aumenta no solo cuando hay divergencias con la ley, sino también en ausencia de ella, como es el caso de varios países de la región.

El rápido despliegue de las *corona-apps* en América Latina es una clara señal de las capacidades existentes en materia de digitalización vinculada a la vigilancia. Aun en las sociedades más vulnerables de la región, estas aplicaciones han logrado desplegarse en tiempo récord. La cuestión de la vigilancia, vía herramientas digitales, es un punto de la agenda local desde hace años, pero la evidencia es todavía escasa como para identificar prácticas con potencial de vulnerar derechos al menoscabar la

privacidad[2]. El despliegue de la pandemia en la región ha evidenciado que la capacidad y la voluntad para desarrollar estos instrumentos es real. Por ello, es muy necesario contemplar los beneficios, así como los costos, de estos desarrollos. Si bien la anonimización y la privacidad de los usuarios es factible de contemplar con diversas aplicaciones y mecanismos de cifrado —aspecto que para algunos constituye la esencia de por qué no estamos ante un dilema de pérdida de privacidad—, el recorrido por el avance de las *corona-apps* muestra que se debe producir una conjunción de factores para que su uso traiga a largo plazo más beneficios que problemas.

Por último, este artículo ha mostrado la carencia de un mecanismo regional que permita armonizar, coordinar y posicionar estos debates para evitar la fragmentación que se da entre sus países. Este mecanismo podría impulsar una visión más integradora de la región que aún tiene que afrontar muchas materias pendientes hacia una agenda digital que acompañe al desarrollo sostenible.

Carolina Aguerre es codirectora del Centro de Estudios en Tecnología y Sociedad de la Universidad de San Andrés en Buenos Aires. *La autora agradece la colaboración del Lic. Iván Kirschbaum en el relevamiento de la investigación.*

[2] La sociedad civil en la región ya alertaba sobre los riesgos de los sistemas de vigilancia masiva implementados a partir de la expansión de distintos dispositivos. En 2019 organizaciones de la sociedad civil alertaron al unísono sobre los riesgos de la implementación de sistemas de reconocimiento facial a partir de su implementación en el transporte público de la ciudad de Buenos Aires.

Referencias bibliográficas

FINANCIAL TIMES (2020): "Coronavirus apps. The risk of slipping into a surveillance state" (28/04/2020). Disponible en: https://www.ft.com/content/d2609e26-8875-11ea-a01c-a28a3e3fbd33.

HUTCHINS, R. M. (2007): "Tied up in Knotts-GPS Technology and the Fourth Amendment", *UCLA Law Review*, *55*, 409.

INDEC (2020): "Informes Técnicos" vol. 4, nº 83, Buenos Aires, Disponible en: https://www.indec.gob.ar/indec/web/Nivel4-Tema-4-26-71.

INTERNET WORLD STATS (2019): "Latin American Internet Usage Statistics". Disponible en: https://www.internetworldstats.com/.

LARA, J. C. (2020): "La pandemia de COVID-19 y la pulsión por la vigilancia estatal", Santiago, derechosdigitales.org. Disponible en: https://www.derechosdigitales.org/14411/la-pandemia-de-covid-19-y-la-pulsion-por-la-vigilancia-estatal/.

RANKING DIGITAL RIGHTS (2019): "Ranking Digital Rights Corporate Accountability Index". Disponible en: https://rankingdigitalrights.org/index2019/.

VELÁSQUEZ, A. (2020): Aplicaciones de rastreo digital de contactos, ¿para qué zapatos si no hay casa? La tecnología al servicio del control de la pandemia", Bogotá, Fundación Karisma. Disponible en: https://web.karisma.org.co/aplicaciones-de-rastreo-digital-de-contactos-para-que-zapatos-si-no-hay-casa/.

ZUBOFF, S. (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Londres, Profile Editions.

Fundación Carolina, mayo 2020

Fundación Carolina
C/ Serrano Galvache, 26.
Torre Sur, 3ª planta
28071 Madrid - España
www.fundacioncarolina.es
@Red_Carolina

ISSN: 2695-4362
https://doi.org/10.33960/AC_30.2020