

CORONA-APP: UNA BOMBA DE TIEMPO PARA AMÉRICA LATINA Y EL CARIBE



Alrededor del mundo, ciertas aplicaciones y API están siendo desarrolladas y/o implementadas por los Gobiernos y/o [compañías](#), para el rastreo de contacto y control del COVID-19. Mediante la presente carta, académicos, expertos y organizaciones, advierten a los Gobiernos de América Latina y el Caribe sobre los riesgos que implica el uso de este tipo de tecnologías y recomiendan analizar su eficiencia e impacto en la región.

Contexto

A **nivel internacional**, se perciben distintas respuestas sobre estas tecnologías:

- En la **Unión Europea** (pese a los altos [estándares de protección de datos y privacidad](#)), expertos y académicos han solicitado a sus respectivos Gobiernos **un debate saludable sobre su uso, por los peligros que ello implica**. En **Bélgica**, por ejemplo, la carta abierta dirigida al Gobierno, promovida por más de 100 académicos, entre ellos [Nathalie Smuha](#), Lode Lauwaert y Massimiliano Simons, ha sido una de las más inspiradoras y contundentes, al indicar que este tipo de

tecnologías “no solo enfrenta problemas jurídicos, sino, también, éticos, sociales, políticos y técnicos (tanto el uso voluntario como el obligatorio)”. Por otro lado, recientemente, países miembros de la UE, apoyados por la Comisión Europea, han desarrollado de modo conjunto una serie de [herramientas y directrices](#) para el uso de este tipo de tecnologías.

- En **Estados Unidos**, los responsables de la salud pública en los Estados más afectados, como Nueva York, Massachusetts y California, además de ciudades como San Francisco y Baltimore, de momento, [han rechazado el uso de tecnologías rastreadoras](#) y se han concentrado en contratar y desplegar ejércitos de personas, con asistencia limitada de tecnología, para rastrear manualmente a los infectados por el virus. Y, como indican algunos funcionarios de la salud, posiblemente, este será el modelo que se usará a nivel nacional.
- En **China, Corea del Sur, Rusia, Israel, Taiwán y Singapur**, han aplicado esta tecnología de forma inmediata y sin cuestionarla. Sin embargo, **Singapur**, que fue uno de los primeros países en usar un aplicativo para rastrear el coronavirus, hace poco sufrió un [importante rebrote de 1111 nuevos infectados](#), al parecer debido a la confianza plena sobre la eficacia de la aplicación, sin tener en cuenta que su eficiencia técnica está condicionada: (i) a que la [mayor parte](#) de la población (o toda) la utilice; y (ii) a que los errores de falsos negativos sean bajos o nulos. A pesar de esto último, actualmente se están volcando de modo fundamental en este aplicativo; así, sus rigurosas leyes y la supuesta ausencia de brecha digital les hace confiar en la supuesta eficiencia técnica de esta tecnología. En **Israel**, por su parte, [la Corte Suprema le ha prohibido](#) a la Agencia de Inteligencia del país el uso de estas aplicaciones para rastrear a las personas infectadas, y además ha mostrado su preocupación sobre el uso de este tipo de tecnologías contra ciudadanos inocentes.

¿Por qué aplicativos que rastrean el COVID-19 podrían representar una bomba de tiempo para Latinoamérica y el Caribe?

La confianza ciega en este tipo de tecnologías podría viabilizar consecuencias devastadoras en América Latina y el Caribe (ALC): (i) a nivel de vidas humanas, debido a que la confianza plena en este tipo de aplicativos podría generar en los ciudadanos una falsa sensación de seguridad, que les haría volcarse a las calles -guiados por información de esta tecnología- poniendo en riesgo su salud/vidas, pese a no existir certeza de su eficiencia técnica (y más en regiones como la nuestra, por las características que en breve explicaremos); y (ii) a nivel de derechos, debido a que podría facilitar violaciones sistemáticas (a corto y/o largo plazo) contra los derechos humanos, protección de datos, privacidad, entre otros (tema sensible y con varios conflictos de interés).

Como ya hemos mencionado, hay riesgo de **falsos negativos y falsos positivos** en el uso de los *corona-apps*. Así, la geolocalización por GPS no suele alcanzar la [precisión necesaria](#) para hacer el rastreo efectivo. Por otra parte, las soluciones con [Bluetooth](#) también vienen siendo cuestionadas en su eficiencia, debido a interferencias, barreras físicas (como paredes, bolsillos, entre otras), y así son susceptibles a dos tipos de errores: (i) falsos negativos, cuando el sistema no detecta un contacto en virtud de interferencias, barreras, etc.; y (ii) [falsos positivos](#), cuando el sistema despliega la localización original del individuo haciendo creer que está próximo a otro sujeto (posiblemente infectado), cuando en realidad están muy lejos el uno del otro, entre otros casos.

Además, Latinoamérica y el Caribe posee características distintivas que, como hemos mencionado, deben ser consideradas:

1. **La brecha digital.** En los países de Latinoamérica y el Caribe, esta brecha es sustancial, haciendo cuestionable y a veces hasta imposible que el aplicativo sea accesible y descargado por la mayoría de la población.

En efecto, de acuerdo con [CEPAL \(Comisión Económica para América Latina\)](#), en el 2016:

*Los registros promedio de ALC en cuanto **al acceso a infraestructuras digitales están bastante por debajo de los del promedio de países de la OCDE.** Por ejemplo, el **27 % de la población** de ALC está cubierta por redes de cuarta generación de **banda ancha móvil (4G)**, frente a 77 % de la población de los países de la OCDE. Dentro de la región se pueden encontrar niveles de desarrollo muy dispares.*

- 2. La desinformación y la crisis institucional.** Como se sabe, la administración pública de algunos países de ALC pasa por crisis institucionales y/o sufre de desconfianza en su gestión, generando opiniones contradictorias en relación a la crisis del coronavirus. Por ejemplo, México y Brasil [viven un caos informacional](#) (que podría extenderse en la región) que genera una grave confusión en sus respectivas poblaciones, las cuales no saben con claridad cómo prevenir la infección del coronavirus, no saben cuán mortífero es este virus e inclusive existen situaciones extremas donde, debido a la desinformación, hay personas que cuestionan la existencia del virus. En escenarios como estos, la desconfianza hacia los Gobiernos implicará un reducido número de instalaciones de las aplicaciones. Por otro lado, existen casos internacionales extremos donde ciertos Gobiernos exigen la instalación obligatoria de este tipo de aplicativos, no siendo esta una solución razonable ni legal, de acuerdo con los estándares internacionales de protección de datos personales y privacidad, pues podrían utilizarse de forma abusiva o para fines de vigilancia, más allá de lo estrictamente necesario para combatir la crisis sanitaria.

¿Cuáles son los problemas respecto a la protección de datos y privacidad de los corona-apps?

Las soluciones tecnológicas conllevan problemas intrínsecos con respecto a la protección de datos y la privacidad. Por ello, las modernas leyes de protección de datos, los estándares internacionales en materia de privacidad y la comunidad académica internacional exigen que se respondan las siguientes preguntas para garantizar el cumplimiento de principios, derechos y garantías fundamentales en esta materia:

- ¿Estas aplicaciones cumplen con los principios de necesidad y proporcionalidad que justifican la recolección de los datos?
- ¿Quién o quiénes tendrán acceso, usarán y/o recolectarán efectivamente los datos de los celulares?
- ¿Cuánto tiempo conservarán los datos? ¿Serán semanas, meses, años? ¿Se cuenta con una cláusula de caducidad para que los datos sean eliminados cuando termine la crisis?
- ¿Qué uso le darán (ya sea el sector público o privado) y cuáles serán las limitaciones o restricciones en su uso?
- ¿El Gobierno está en posición de asegurar la protección de los datos?
- ¿Qué protocolo será utilizado por el sistema: el centralizado o el descentralizado? ¿Por qué?
- ¿Será de código abierto? ¿Permitirán auditorías independientes para garantizar la seguridad y la transparencia?
- ¿El sistema elegido es el más confiable para los ciudadanos?
- ¿Cómo se sabrá si se dejará de usar/rastrear a las personas una vez superada esta pandemia? ¿Cómo el gobierno asegurará que los datos no serán transferidos o vendidos a terceros?

La transparencia es importante; en ese sentido, es relevante que se responda a estas preguntas, porque el uso de los datos, dependiendo de quién los tenga, el sistema que use, entre otros factores, pueden condicionar/afectar la vida personal, profesional y económica del ciudadano, e inclusive dañar la frágil democracia en nuestra región.

¿Qué pueden hacer los Gobiernos de Latinoamérica, el Caribe y la sociedad?

Durante el desarrollo de la pandemia, los *corona-apps* no han evidenciado seguridad plena sobre su efectividad a nivel internacional, y posiblemente tampoco lo harán en Latinoamérica y el Caribe, más aún debido a las características socioeconómicas y contextuales (como la de la brecha digital y la desinformación). Por lo tanto, consideramos relevante que estos temas sean seriamente observados no solo por los Gobiernos, sino también por la sociedad en sus diferentes representaciones (sociedad civil, académicos, expertos, empresarios, comunidad técnica, etc.).

De este modo, hacemos las siguientes **recomendaciones**:

- 1. Crear un grupo independiente y multidisciplinario de profesionales que colabore en el desarrollo de medidas diversas, sólidas y estratégicas, y que ayuden a dar solución a este problema de modo más amplio y no solo estar centrados en la tecnología para dar solución a esta crisis.** El grupo debe incluir a epidemiólogos, científicos sociales, biólogos, filósofos, abogados, psicólogos, especialistas en tecnología y ética, etc., para ayudar a actuar más contundentemente en el establecimiento de medidas contra el COVID-19. Y es que, si solo se tiene en cuenta la opinión de un sector reducido y no variado de profesionales, lamentablemente, se podrían generar medidas sesgadas o deficientes, que favorecerían el rebrote vírico. Por ejemplo, la ausencia de un equipo multidisciplinario podría generar políticas desventajosas para las poblaciones más vulnerables y desfavorecidas económicamente, así como para las personas mayores, entre otras, carentes de celulares o sin conocimientos para usarlos, las cuales no serían tomadas en cuenta, ni por error, poniéndose en riesgo sus vidas, y con ello institucionalizando políticas públicas vulneradoras de derechos fundamentales.
- 2. Que el debate sobre el uso de los *corona-apps* incluya a todos los sectores relevantes de la sociedad.** En este punto, sobre todo, sugerimos que se preste

atención a los problemas que la confianza plena en su uso puede representar para los ciudadanos, tales como problemas éticos, jurídicos, sociales, políticos y, el más preocupante a corto plazo, los problemas técnicos de seguridad, eficiencia y eficacia, que podrían poner en riesgo la vida de muchas personas. Dicho debate o análisis permitirá entender hasta qué punto pueden confiar en dicha tecnología y la importancia y posición que se le debe dar, en comparación o en conjunción con otras medidas, en la lucha contra esta pandemia.

- 3. Garantizar la transparencia de la información.** A partir de la creación de mesas de trabajo multidisciplinarias y la transparencia, los Gobiernos deben construir confianza en los ciudadanos para que las medidas que adopten sean eficientes para combatir la pandemia. Para cumplir con ese objetivo, las autoridades tendrían que: (i) garantizar el cumplimiento de las leyes de acceso a la información pública, y publicar informes con estadísticas oficiales del estado de la crisis; (ii) realizar evaluaciones del impacto de la tecnología sobre los derechos humanos; y (iii) permitir auditorías independientes en el desarrollo, implementación y resultados de las políticas adoptadas o a adoptar, entre otras medidas similares.

Finalmente, esperamos que los Gobiernos de Latinoamérica y el Caribe puedan percibir esta iniciativa como un mensaje de preocupación y de solidaridad que les advierta de los errores y aciertos de la comunidad internacional, y tomen en cuenta esta propuesta.

NOTA:

1. Para contactar con los intervinientes de la carta, escribir a investigacion.lac@protonmail.com

2. Registrada en ResearchProof.

Autores:

- Karin Tafur. Especialista en Legal Tech y analista jurídica de nuevas tecnologías e inteligencia artificial (Perú).

- Thiago Guimarães Moraes. Especialista en derecho y tecnología, protección de datos y derechos autorales (Brasil).
- Gaspar Pisanu. Abogado especialista en derechos humanos y tecnología, y analista de políticas públicas (Argentina).

Colaboradores:

- Nathalie Smuha (Bélgica).
- Gustavo Gómez (Uruguay).
- Verónica Arroyo (Perú).
- Christian Perrone (Brasil).
- Erick Leddy García (Perú).

***[El número de firmantes que apoyan esta iniciativa sigue incrementándose, esperamos que tú también puedas unirte a esta noble causa].