BID
Banco Interamericano de Desarrollo

¿Es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia?

Sector Social

Marcelo Cabrol
Ricardo Baeza-Yates
Natalia González Alarcón
Cristina Pombo

DOCUMENTO PARA DISCUSIÓN Nº
IDB-DP-00763

Abril 2020

¿Es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia?

Marcelo Cabrol
Ricardo Baeza-Yates
Natalia González Alarcón
Cristina Pombo

Abril 2020

BID
Banco Interamericano de Desarrollo

¿Es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia?[1]

Marcelo Cabrol (BID), Ricardo Baeza-Yates (Northeastern University), Natalia González Alarcón (BID) y Cristina Pombo (BID)

La iniciativa fAIr LAC[2] del Banco Interamericano de Desarrollo (BID) promueve el uso ético[3] y responsable de los datos y de los sistemas basados en la inteligencia artificial, para que sean centrados en la persona bajo principios de equidad. Para esto, todos los actores del ecosistema deben respetar, entre otros, los valores democráticos de los ciudadanos tales como la privacidad y la protección de los datos. Aun en tiempos de máximo riesgo para la salud pública, hay que hacer compatible la elección individual entre la privacidad personal y la elección social y del bienestar de todos. Esta es una cuestión ética de primer orden especialmente relevante con la pandemia actual y por ello es necesario discutirla a fondo.

En la lucha contra el COVID19, miles de millones de datos personales geo-localizados están siendo utilizados por diferentes países alrededor del mundo con el fin de "aplanar la curva" de contagio, para restablecer la circulación de las personas y gestionar mejor el distanciamiento físico entre personas. Nos referimos a los sistemas de vigilancia que varios gobiernos han empezado a utilizar para **seguir o rastrear personas y sus contactos físicos** *(contact-tracing)*. A través de estas herramientas digitales los gobiernos buscan rastrear el movimiento de personas infectadas, identificar a aquellos que pueden haber estado expuestos al coronavirus, rastrear sus contactos físicos para alertar y advertir de los riesgos en el futuro, hacer seguimiento de las órdenes de distanciamiento físico, publicar mapas que identifiquen áreas de riesgo y de esta forma, lograr implementar y hacer cumplir las medidas para contener el contagio. Este uso de la tecnología es polémico dadas las implicaciones que tiene en cuanto a riesgos en privacidad y las decisiones que están tomando algunos países al respecto. Si entendemos los datos como un bien público (no rival y no excluyente) necesario para mejorar y acelerar la respuesta en medio de una pandemia, ¿se justifica entonces la flexibilización de los estándares de privacidad? ¿justifica el fin último de rastreo y control del contagio

1 Los autores agradecen los comentarios de Marcelo D'Agostino, Asesor Senior en Sistemas de Información y Salud Digital en Organización Panamericana de la Salud/OMS, Alejandro Pardo del BID Lab, Jennifer Nelson y Luis Tejerina de la división de Salud y Protección Social del BID, Pablo Picón y Roberto Sánchez del Sector Social del BID.

2 Como resultado del creciente interés de la región en usar la inteligencia artificial para la solución de problemas sociales, y los retos que esto supone, en 2019 nace fAIr LAC con el objetivo de promover su uso ético y responsable para mejorar la provisión de servicios sociales.

3 Todo lo que se enmarque en los principios éticos que definió la OECD.

como medida de asegurar la salud de todos y reestablecer cierta normalidad social una posible vigilancia intrusiva de los gobiernos?, y en caso de que así sea, ¿existen condiciones que mitiguen los riesgos sobre la privacidad a los que se ven expuestos los ciudadanos?

Rastreando personas y sus contactos físicos

Según la OMS, los **sistemas de rastreo de personas y sus contactos físicos** funcionan en tres pasos (siguiendo la manera tradicional de hacerlo a través de personal de salud pública especializado y entrevistas personales):[4]

1. Con los casos confirmados, identifica aquellos con los que el paciente infectado tuvo contacto,
2. Registra los posibles contactos físicos de los pacientes infectados y los contacta, y
3. Hace seguimiento con el listado de contactos ya sea para hacerles una prueba o para advertirles que estuvieron en contacto con alguien infectado.

Estas herramientas de rastreo de personas se han convertido en parte de la estrategia de gestión de la pandemia de varios países asiáticos que han sufrido la primera oleada de esta y está tomando fuerza entre varios grupos de expertos[5] quienes han alcanzado un importante grado de consenso sobre su efectividad para frenar el contagio sin tener que forzar a la población a confinamientos estrictos. Esto se debe a que la aplicación de estas herramientas permitiría a los usuarios saber su exposición potencial con una persona infectada, rastrear su historial de contactos físicos o identificar zonas de riesgo y de esta forma tomar acciones apropiadas tales como el distanciamiento físico. El efecto sería la reducción de la tasa de contacto más rápidamente de los casos potenciales (expuestos al virus) ya que estos serán eliminados de la cadena de contacto. Una debilidad de estas aplicaciones es que hay un gran porcentaje de casos asintomáticos, estimados entre 18% y 42%, que pueden no ser detectados y que podrían ser el principal foco de contagio.

Este tipo de intervenciones de salud pública pueden estar respaldadas por diferentes tecnologías. El estado de Massachusetts ha decidido irse por el tradicional rastreo de personas de forma manual, contratando a más de 1000 personas para contactar a las personas diagnosticadas y de esta forma hacer el rastreo. Sin embargo, el proceso toma demasiado tiempo para que el rastreo de contactos sea efectivo.

En Corea del Sur rastrean vía GPS para tener control de los infectados por COVID-19

El caso de Corea del Sur está siendo muy estudiado debido al éxito que ha tenido en el control de la pandemia. El gobierno ha utilizado diferentes tecnologías para prevenir y controlar el contagio, pero la base de su éxito ha sido una capacidad sanitaria elevada al abordar la masificación del testeo de COVID-19 a la población, en conjunto con una capacidad de gestión digital que ha permitido el seguimiento riguroso a través de rastreo vía GPS de los infectados y en cuarentena para identificar cualquier persona con la que los portadores del virus hayan estado en

4 La OMS tiene su propio app, Go.Data (sin IA) para hacer esto – http://socialdigital.iadb.org/en/solutions/go-data-covid-19

5 Como el grupo de expertos de Massachusetts Institute of Technology que están desarrollando Safe Paths, así como el grupo de expertos de diversas especialidades de Oxford University que analizan las implicaciones y requerimientos para el uso de rastreo por contacto.

contacto. Hasta el 25 de marzo, el país ha realizado más de 350.000 pruebas, la cantidad más alta per cápita del mundo. Por su parte, otros países asiáticos están recurriendo al uso de pulseras rastreadoras de alta tecnología para monitorear los casos positivos. Más de 20.000 viajeros que llegaron a Hong Kong recibieron pulseras que el gobierno adquirió para monitorear el movimiento de las personas en cuarentena.

Singapur por su parte lanzó TraceTogether el 20 de marzo, 5 días después había sido descargado por 735.000 personas, aproximadamente el 13% de la población. Esta aplicación a diferencia de las anteriores funciona como una red computacional distribuida persona-a-persona usando *Bluetooth* a una corta distancia. Esto permite que no haya un control central que reciba todos los datos y por ende se protege la privacidad individual. Taiwán utiliza un enfoque diferente, rastreando los teléfonos de las personas en cuarentena utilizando datos de antenas de teléfonos celulares. Si detecta a alguien fuera de límites, les envía un mensaje de texto y alerta a las autoridades.

Ahora, el principal desafío del despliegue de estas aplicaciones son los límites de privacidad y la gestión del consentimiento informado.[6] En un sistema respetuoso de la privacidad, el individuo propietario de los datos personales debe entender y aceptar el uso o tratamiento que se le dará a su información, y con el uso de rastreo de contactos estos riesgos existen tanto para el individuo.

Debido a que la aplicación necesita analizar las trayectorias de los últimos 15 días de **los pacientes portadores** para identificar otras personas en potencial riesgo, estos corren el mayor riesgo de que su privacidad sea expuesta. Aunque su información personal no se publique explícitamente, podrían ser identificados si se publica un conjunto limitado de datos de ubicación, como lo hicieron en el caso de la paciente número 31 en Corea del Sur. Este problema no es nuevo y ya ocurre con datos provenientes de aplicaciones de juegos que se pueden comprar y que han permitido identificar a personas o seguir el rastro de agentes de seguridad de jefes de estado.

En China los códigos QR identifican el riesgo de contagio de las peronas

Los **usuarios de las aplicaciones** también están en riesgo ya que su ubicación es utilizada para establecer si se han cruzado con un paciente diagnosticado. El problema acá es cuando un tercero, generalmente el gobierno, accede a los datos de ubicación. Por ejemplo, Alipay App, la aplicación china usada en más de 200 ciudades para ayudar a los ciudadanos a identificar los síntomas y su riesgo de contagio, se basa en un código QR donde cada usuario recibe uno de los tres colores: verde, amarillo o rojo, según su ubicación, información básica de salud e historial de viajes. Los problemas son varios. Primero, falta de información,[7] ni la compañía ni el gobierno han explicado en detalle cómo el sistema clasifica a las personas en cada color, lo cual causa temor entre la gente que recibe la orden de aislarse sin saber el por qué. Segundo, falta de transparencia sobre cómo están usando sus datos personales y dónde se están almacenando. La aplicación solicita detalles de contacto, información del pasaporte, viajes recientes y una certificación médica. De acuerdo con un análisis del New York Times, todo parece indicar que la apli-

6 El acceso a datos de ubicación de los individuos depende de la regulación vigente en cada país o en cada estado. Ver caso de EE.UU. acá.

7 Para mayor detalle revisar página 25 de la nota técnica de fAIr LAC aquí.

cación comparte información con la policía, estableciendo una nueva forma de control social automatizado que podrían persistir incluso después de la epidemia. Por otro lado, Apple y Google han decidido unir esfuerzos para que todas las aplicaciones de rastreo recomendadas por los gobiernos se instalen automáticamente cuando se actualice el sistema operativo del teléfono.

Finalmente, los riesgos para el **público en general** radican en que los usuarios y los no usuarios están conectados a través de relaciones sociales y proximidad espacial. Si se revela la identidad de un familiar o amigo como portador del virus, pueden ocurrir estigmatizaciones y repercusiones sociales. Considere que usted está en cuarentena por la enfermedad, ¿deben saber sus vecinos esto? Ya ha habido profesionales de la salud a los que se les ha pedido irse a vivir temporalmente en otro lugar pues sus vecinos tienen miedo a contagiarse.

Ahora, ¿qué debería primar en el uso de los datos para la vigilancia de la pandemia?

En este dilema entre salud y privacidad, ¿cómo percibe la población de América Latina y el Caribe estas medidas durante una pandemia? Aun no lo sabemos. Un estudio realizado en el 2006, mostró una percepción poco favorable de las personas sobre el uso de varias medidas durante un posible brote de la enfermedad en las cuatro regiones incluidas (EEUU, Hong Kong, Taiwán, Singapur). Es importante tener conversaciones con la población e incluirles para que puedan participar en la decisión sobre su utilización o no.

Algunas de estas aplicaciones han diseñado salvaguardias de privacidad aplicando el principio de *"privacy by design"*, conciliando con claridad el derecho a la privacidad con las necesidades de control de la pandemia. TraceTogether de Singapur afirma que no recopila ni utiliza datos de ubicación de ningún tipo, y no accede a la lista de contactos ni a la libreta de direcciones de los usuarios. Solo utiliza datos de bluetooth para establecer un contacto y no almacena información de manera centralizada sobre dónde ocurrió el contacto. Adicionalmente el gobierno está en el proceso de abrir el código lo que permitirá ser auditado por otros.

La tecnología Bluetooth es capaz de alertar sobre posibles contagios cercanos sin dejar rastro geolocalizador

De acuerdo con Ramesh Raskar, investigadora del MIT Media Lab y quien lidera el desarrollo de Private Kit: Safe Paths, una aplicación de rastreo de contactos que busca proteger la privacidad de los usuarios, afirma que con Safe Paths las personas infectadas pueden borrar ubicaciones que puedan ser sensibles o revelar su identidad. Además, los datos de ubicación de todos los usuarios que no están infectados se guardan únicamente en el teléfono, no en el servidor. De esta forma los usuarios serán los únicos que sabrán si se cruzaron o no con un paciente infectado. Otra iniciativa similar, también en el MIT, usa Bluetooth para alertar a las personas sin revelar la identidad de ellas.

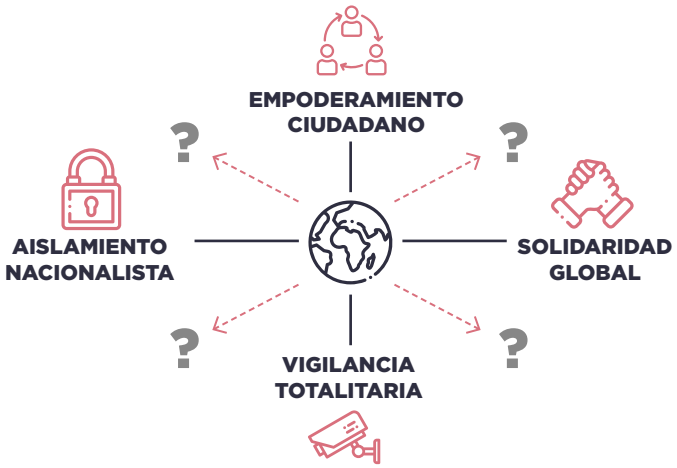
Por su parte, Europa, la región con las leyes de privacidad de datos más estrictas del mundo, ha empezado a tomar decisiones al respecto. De acuerdo con la Junta Europea de Protección de Datos, los datos de ubicación solo pueden ser utilizados por el operador cuando se hacen anónimos o con el consentimiento de los usuarios. Sin embargo, la RGPD permite que durante una epidemia las autoridades competentes puedan procesar datos personales de acuerdo con las legislaciones naciona-

les, pues en circunstancias excepcionales no es necesario el consentimiento previo.[8] La canciller alemana, Angela Merkel, anunció el desarrollo del Pan-European Privacy Preserving Proximity Tracing (PEPP-PT), una aplicación de rastreo de personas que **protege los datos y no almacena la ubicación de sus usuarios**. Al igual que TraceTogether, utilizará Bluetooth para registrar la proximidad de un usuario con otros con mucha precisión, pero con menos alcance que GPS, para que las personas reciban un mensaje si han estado en contacto con un portador del virus. Tanto Bélgica como Austria, están usando bases de datos de empresas de telecomunicación combinadas con los datos de salud, bajo la supervisión de las autoridades correspondientes para garantizar el uso **de datos agregados y anónimos** para evaluar cómo se propaga el virus y qué áreas son de alto riesgo. En Alemania, Deutsche Telekom ha proporcionado datos al Instituto Robert Koch, la agencia de salud pública del gobierno, de forma agregada. Igualmente, el gobierno británico está en conversaciones con operadores de telefonía celular sobre el acceso a datos similares. Un estudio reciente encontró que el 51% de las personas encuestadas en el Reino Unido estaban preocupadas por la privacidad de sus datos a medida que aumenta el uso de IA, lo cual es más relevante en el sector de la salud, debido a que la información que se comparte a través de aplicaciones de rastreo de personas es altamente sensible.

Conclusiones

Un ensayo publicado por el historiador israelí Yuval Harari describe los modelos de gestión del dilema privacidad-salud en un doble eje: el primero establecido por la "vigilancia totalitaria" vs "empoderamiento de los ciudadanos" y el segundo entre el "aislamiento nacionalista" y la "solidaridad global". El cuadro siguiente sitúa el mundo, según él, "tras el coronavirus", lo que da una buena idea de las preguntas que este debate sugiere al menos en lo que dure el tiempo de control y gestión de la pandemia.

Dónde se situará el mundo tras el coronavirus



Fuente: adaptación gráfica de Mario Tascón.
Basada en el artículo de Yuval Noah Harari (autor de Sapiens) en el Financial Times.

Las diferentes alternativas que los gobiernos tienen para rastrear y geo-localizar a sus ciudadanos la tecnología que usan tienen implicaciones distintas en la privacidad de las personas. Algunas de estas aplicaciones exceden los estándares de

8 Adicionalmente, estas medidas deben ser estrictamente limitadas a la duración de la emergencia, en este caso de la pandemia.

privacidad que los gobiernos tienen bajo condiciones normales en el uso de los datos de los ciudadanos. El debate es determinar en qué condiciones, si las hay, un gobierno debería tener acceso a tales datos, bajo qué circunstancias y durante cuánto tiempo. ¿Es necesario un mayor seguimiento de la ubicación para proteger la salud pública en medio de una pandemia?, o ¿es una vigilancia intrusiva del gobierno?, ¿se pueden desarrollar herramientas que minimicen los riesgos de privacidad?, ¿exceder límites en privacidad erosiona la confianza en las autoridades? ¿Cuáles son los mejores prácticas y políticas que se debe aplicar – durante y después de la pandemia?, ¿es posible que los ciudadanos "cedan" sus datos solo mientras dure la pandemia? ¿cuándo terminan las atribuciones excepcionales y que se hace con los datos recopilados? Se debe hacer notar que las respuestas a estas preguntas son distintas de una cultura a otro e incluso de un país a otro, pues dependen del nivel de democracia y la confianza que la gente tiene en sus gobiernos.

Para contestar estas preguntas y resolver este debate debemos tener en cuenta que las aplicaciones de rastreo de personas deben tener tanto requerimientos sociales debido a los aspectos éticos, como requerimientos tecnológicos debido a los objetivos que se quieren conseguir. Para ellos tenemos que considerar los siguientes factores sociales y tecnológicos, entre otros:

- **Es una cuestión ética mantener el equilibrio entre la privacidad individual, la libertad de movimientos y el interés colectivo de la salud**. Sin embargo, cada entorno requerirá la tecnología más adecuada a sus circunstancias particulares. Soluciones como TraceTogether han tenido éxito porque la sociedad de Singapur se ha comprometido en su uso y gracias a su adopción rápida, ha cumplido su función. Varios países europeos han optado por utilizar información masiva de sus operadores de telecomunicaciones cruzada con los sistemas de salud, otros sin embargo optan por alternativas más respetuosas con la privacidad. El mismo debate recién ha comenzado en Estados Unidos.
- **Hay que considerar las consecuencias de pedirle a las personas que voluntariamente se hagan una prueba y que hagan pública su situación**, especialmente a minorías o incluso en algunos países a grupos perseguidos por su raza, religión u orientación sexual. No se puede usar la salud para obtener información que podría ser usada para atentar con los derechos humanos.
- Hay **países en los que todavía hay parte de la población sin tecnología móvil adecuada**. Estas áreas requerirán soluciones específicas considerando además factores socioeconómicos como la existencia de economía informal que pueden complicar la elección de las tecnologías más adecuadas.
- Otro elemento clave es **la efectividad de la solución tecnológica**. Una vez decidido qué modelo tecnológico es el más adecuado para las circunstancias de cada país, puede que existan ya alternativas desarrolladas por otros países y probadas que están disponibles. Aprovechar soluciones ya establecidas reducirán los riesgos de implantación y agilizarán su adopción.
- Hay que **explorar en mayor profundidad el uso de protocolos criptográficos y/o privacidad diferencial**, para permitir proteger mejor la privacidad de las personas al mismo tiempo que permiten gestionar los datos que se necesitan para controlar una epidemia. La pandemia no nos ha dado tiempo para hacer esto como se debe.

La **falta de privacidad** tiene además otra consecuencia, **erosiona la confianza** en el Estado por parte de la ciudadanía. Más aún, **la falta de transparencia** de los gobiernos en el uso de los datos personales, combinado con la **falta de información** de cómo estas aplicaciones toman decisiones, como es el caso de China con Alipay, disminuyen la confianza pública. Aunque la ciudadanía gradualmente se va acostumbrando a convivir con la era de los datos masivos y se conocen numerosas historias de éxito, también hay casos de falta de transparencia y mal uso de los datos, los cuales también afectan la confianza.

Todo lo anterior evidencia la necesidad de priorizar la privacidad de las personas y por ende los gobiernos deben propender al uso de datos agregados y anonimizados, para que así también puedan ser abiertos, tal como se ha propuesto recientemente en Chile. Por otro lado, la mayoría de las personas cada vez que instala una aplicación cede parte de su privacidad, sin saber ni siquiera que parte es, pues no lee las condiciones y términos de uso que acepta sin pensar. Si este es el caso, puede que perder algo que en realidad ya se ha perdido, no sea relevante para muchas personas, sobre todo las más jóvenes. ¿Puede ser viable entonces relajar temporalmente la privacidad de los datos en estados de alarma?

Por último, es fundamental evaluar **la calidad de los datos** que están siendo usados para contener o informar sobre los efectos del COVID-19. En ausencia de buenos y suficientes datos, los resultados van a ser débiles, erróneos y, teniendo en cuenta que estamos tratando de información de salud, pueden ser catastróficos (*garbage in, garbage out)*. De hecho, si los datos no son de buena calidad o estandarizados (indicadores comparables), en la mayoría de los casos es mejor no tenerlos. Esto también afecta negativamente la credibilidad y confianza hacia la tecnología y hacia sus promotores que, en este caso, son los gobiernos. Un tema adicional es como estos datos y cuanto tiempo, pueden o deben ser archivados para el futuro.

Si volvemos atrás, al título de este ensayo, vemos que la pregunta que hacíamos plantea una **falsa dicotomía**, ya que como hemos visto es posible usar bien la tecnología para no tener que renunciar a toda nuestra privacidad, sin tampoco renunciar a lidiar lo mejor posible con una pandemia. Al final, como casi todas las cosas de la vida, particularmente en la salud, la solución no está en los extremos, sino en el consenso, trabajo en red y búsqueda de soluciones colectivas. La pandemia no nos ha dado tiempo para hacer esto como se debe y ya hay voces que demandan que la privacidad sea la norma.