



Rastreo y seguimiento del COVID-19: protección de la privacidad y los datos en el uso de aplicaciones y biometría

Actualizado el 23 de abril de 2020

Mensajes clave

- Las tecnologías digitales, en particular las aplicaciones móviles y biométricas, se están adoptando de manera innovadora para mejorar la eficacia de las respuestas gubernamentales de primera línea frente al COVID-19.
- La información y las tendencias resultantes son invaluablees para los gobiernos que busquen realizar un seguimiento de los brotes de COVID-19, advertir a las comunidades vulnerables y comprender el impacto de políticas públicas como el distanciamiento social y el confinamiento.
- El uso de información personal puede permitir al público identificar mejor posibles casos de contagios de COVID-19 y realizar un seguimiento de su propagación a lo largo del tiempo. Sin embargo, las soluciones digitales actuales para el monitoreo y la contención tienen diferentes alcances en términos de privacidad y protección de datos.
- Se deben integrar soluciones totalmente transparentes y confiables para la conservación de la privacidad en las tecnologías desde su diseño, para equilibrar los beneficios y los riesgos asociados con la recopilación, el procesamiento y el intercambio de datos personales. Los datos deben conservarse sólo durante el tiempo que sea necesario para cumplir con el propósito específico para el que fueron recopilados.



Los gobiernos están colaborando con los proveedores de servicios de telecomunicaciones para acceder a los datos de geolocalización y rastrear los movimientos de la población

A medida que el COVID-19 sigue afectando vidas y sacudiendo la economía mundial, los gobiernos están buscando urgentemente herramientas innovadoras para informar las políticas públicas y hacer frente a la crisis. Están surgiendo soluciones digitales basadas en datos de geolocalización para ayudar a las autoridades a supervisar y contener la propagación del virus. Algunas de estas soluciones son alimentadas por registros de datos de llamadas móviles (CDR), es decir, datos producidos por proveedores de servicios de telecomunicaciones en llamadas telefónicas u otras transacciones de telecomunicaciones, que proporcionan información valiosa sobre los movimientos de la población. A medida que los operadores de redes prestan sus servicios a segmentos sustanciales de la población en naciones enteras, los movimientos de millones de personas se pueden medir casi en tiempo real y con gran precisión de espacio y tiempo. La información y las tendencias resultantes son invaluable para los gobiernos que buscan realizar un seguimiento del brote de COVID-19, advertir a las comunidades vulnerables y comprender el impacto de políticas públicas como el distanciamiento social y el confinamiento.

Los proveedores de telecomunicaciones de varios países de la OCDE han comenzado a compartir datos de geolocalización basados en CDR con los gobiernos en un formato agregado y anónimo. Por ejemplo:

- El proveedor alemán de telecomunicaciones Deutsche Telekom proporciona datos anónimos de "flujos de movimiento" de sus usuarios al Instituto Robert-Koch, un instituto de investigación y agencia gubernamental responsable del control y la prevención de enfermedades.
- El ["Five Point Plan"](#) del Grupo Vodafone para abordar el COVID-19 incluye proporcionar a los gobiernos grandes conjuntos de datos anónimos (como un mapa de calor agregado y anónimo para la región de Lombardía, por citar un ejemplo) para ayudar a las autoridades a comprender mejor los movimientos de la población.
- La Comisión Europea está colaborando actualmente con ocho operadores europeos de telecomunicaciones para obtener de ellos datos de geolocalización móvil agregados y anónimos, con el fin de coordinar las medidas de seguimiento de la propagación del COVID-19. Para abordar los problemas de privacidad, los datos se eliminarán una vez que la crisis haya terminado.

También se están lanzando nuevas aplicaciones móviles para el "seguimiento" del COVID-19

Las aplicaciones móviles de asesoramiento sanitario ya constituyen una parte importante del ecosistema de salud móvil y han demostrado ser eficaces para prevenir, dar un diagnóstico temprano (por ejemplo, comprobando síntomas) y conectar a los usuarios con servicios de salud locales y unidades de emergencia. Ahora, están surgiendo nuevas aplicaciones orientadas al consumidor y destinadas al seguimiento del COVID-19. Estas aplicaciones se desarrollan cada vez más como código abierto y son el producto de asociaciones de empresas de tecnología, organizaciones académicas, personal médico y autoridades públicas, que son en última instancia responsables de su financiamiento, desarrollo e implementación. Aunque no necesariamente capturan a toda la población (por ejemplo, a las personas de la tercera edad que pueden no tener o utilizar teléfonos inteligentes) y pueden presentar errores (al no distinguir entre personas que residen en un mismo hogar y las que se encuentran en residencias vecinas, por ejemplo), estas aplicaciones proporcionan otra herramienta para que los gobiernos monitoreen y contengan el virus. Entre las más citadas se encuentran:



- **[TraceTogether](#)**: desarrollada por la Agencia Gubernamental de Tecnología de Singapur (GovTech) en colaboración con el Ministerio de Salud, esta aplicación utiliza Bluetooth para rastrear a las personas que han estado expuestas al virus. Esta información se utiliza para identificar contactos cercanos en función de la proximidad y duración de un encuentro entre dos usuarios. A continuación, la aplicación alerta a aquellos que entran en contacto con alguien que ha dado positivo o tiene alto riesgo de ser contagioso. Una vez que se sospecha o se confirma que una persona está infectada, se puede optar por permitir que los hospitales, el Ministerio de Salud y terceros accedan a los datos de la aplicación para ayudar a identificar los contactos cercanos. Singapur planea que el protocolo subyacente de preservación de la privacidad para el intercambio de datos sobre el cual está basado TraceTogether esté disponible en código abierto.
- **[Pan-European Privacy-Preserving Proximity Tracing](#)**: más de 130 científicos, tecnólogos y expertos de ocho países europeos, entre ellos Francia, Alemania e Italia, participaron en una iniciativa sin ánimo de lucro que desarrolló una aplicación de código abierto para analizar las señales de Bluetooth entre teléfonos móviles y detectar usuarios que han estado muy cerca unos de otros. La aplicación almacena temporalmente los datos cifrados localmente y, si los usuarios más tarde dan positivo al COVID-19, la aplicación puede alertar a todo aquel que haya estado alrededor de la persona infectada en días anteriores, protegiendo a su vez todas las identidades de los usuarios.
- **La aplicación de seguimiento de Corea**: financiada por el gobierno coreano, la aplicación “seguridad en la auto-cuarentena” es utilizada por las autoridades para proporcionar información sobre el COVID-19 a la población – incluyendo directrices para la cuarentena – así como para prevenir posibles violaciones de órdenes de auto-cuarentena. La aplicación también se puede utilizar para la prevención a través del auto-chequeo de síntomas y para la presentación de informes voluntarios de salud a las autoridades de atención médica. Los datos recogidos no se comparten con terceros.
- **[C-19 COVID Symptom Tracker](#)**: desarrollada en el Reino Unido por una asociación de médicos y científicos del King's College London, una empresa de ciencia de datos de salud derivada de esa institución, y el Instituto Nacional del Centro de Investigación Sanitaria en los hospitales Guy's y St Thomas', el objetivo de esta aplicación es frenar el brote de COVID-19 ayudando a los investigadores a identificar: i) la rapidez con la que el virus se está propagando en diferentes áreas; ii) zonas de alto riesgo en el Reino Unido; y iii) quién está en mayor riesgo, mediante una mejor comprensión de los síntomas relacionados con las condiciones de salud subyacentes. Según los investigadores, los datos del estudio pueden revelar información esencial sobre los síntomas y el progreso de la infección en diferentes personas. La aplicación también puede ayudar a los investigadores a entender por qué algunas personas desarrollan síntomas más graves – o incluso mortales – mientras que otras presentan sólo síntomas leves a raíz del COVID-19.
- **[Apple y Google](#)** también lanzarán una interfaz de programación de aplicaciones (API, por sus siglas en inglés) para permitir la interoperabilidad entre dispositivos Android e iOS al utilizar aplicaciones diseñadas por las autoridades de salud pública. Los usuarios podrán descargar estas aplicaciones a través de sus respectivas tiendas de aplicaciones. Las dos empresas también trabajarán juntas para permitir una plataforma de rastreo de contactos más amplia basada en tecnologías Bluetooth mediante la creación de esta funcionalidad en las plataformas subyacentes. Esta solución permitiría a más personas participar en caso de que así lo decidan y podría eventualmente mejorar la interacción con un ecosistema más amplio de aplicaciones y autoridades de salud gubernamentales.

Las aplicaciones de rastreo pueden incorporar diferentes grados de privacidad y protección de datos

El uso de aplicaciones de recopilación de datos de geolocalización puede permitir el intercambio de datos con protecciones de privacidad explícitas integradas, y permitir a los usuarios dar su consentimiento explícito e informado para la recopilación y el intercambio de sus datos personales (suponiendo que el uso de la



aplicación no es obligatorio). Por ejemplo, la aplicación TraceTogether de Singapur tiene una serie de medidas para salvaguardar la privacidad, entre ellas no recopilar ni utilizar datos de geolocalización y almacenar los registros de datos de forma cifrada. Para proteger la privacidad de sus usuarios, la aplicación paneuropea cifra los datos y anonimiza la información personal. Además, como dos teléfonos nunca intercambian datos directamente y los alias de los usuarios se cambian con frecuencia, es prácticamente imposible revelar la identidad de los usuarios.

Sin embargo, la gama de datos personales que estas aplicaciones recopilan, procesan y comparten puede ser muy amplia y difícil de entender para los usuarios. En muchos casos, las aplicaciones siguen ejecutándose en segundo plano incluso cuando el dispositivo no está en uso. Algunas aplicaciones también pueden intercambiar información con otras aplicaciones a través APIs, generando información más detallada. Si bien la Organización Mundial de la Salud (OMS) elogió las amplias medidas de rastreo de Corea, algunos usos por parte de las autoridades locales designadas para la recopilación de datos a través del Sistema de Apoyo a la Investigación Epidemiológica sobre los movimientos de personas con casos confirmados han suscitado preocupaciones con respecto a la privacidad de los usuarios. En respuesta, el gobierno coreano publicó recientemente normativas relacionadas con la divulgación de los movimientos de personas con casos confirmados – basadas en la Ley de Control y Prevención de Enfermedades Infecciosas aprobada en 2015 – según las cuales no se permite divulgar ninguna información específica del usuario.

Aprovechar los datos biométricos acarrea beneficios y desafíos

El reconocimiento facial ha sido una de las biometrías más utilizadas en varios países para monitorear la propagación del COVID-19. El reconocimiento facial permite a las autoridades reducir el uso de tecnologías de identificación que requieren contacto físico (como escaneos de iris y huellas dactilares). También se puede complementar con otras tecnologías, incluidas las imágenes térmicas potenciadas con inteligencia artificial, para realizar un mejor seguimiento de los ciudadanos que pudieran dar positivo al COVID-19.

En Polonia, el gobierno ha lanzado una aplicación biométrica para teléfonos inteligentes que verifica que las personas infectadas con COVID-19 permanezcan en cuarentena. En la República Popular China (en adelante "China"), el reconocimiento facial se ha utilizado para evitar que viajen los ciudadanos que pudieran estar infectados con COVID-19. Además, las empresas en China han desarrollado una tecnología que podría permitir al gobierno identificar con éxito a las personas incluso cuando llevan máscaras. En la Federación de Rusia, se utilizan sistemas de reconocimiento facial para rastrear a las personas que no respetan la cuarentena obligatoria.

Sin embargo, el uso de la biometría (incluido el reconocimiento facial) en respuesta al COVID-19 plantea una serie de preocupaciones de privacidad y seguridad, especialmente cuando estas tecnologías se utilizan en ausencia de una normativa específica o sin consentimiento plenamente informado y explícito. Asimismo, las personas pueden tener problemas para ejercer una amplia gama de derechos fundamentales, que incluyen el derecho de acceso a sus datos personales, el derecho a borrar esos datos y el derecho a ser informados sobre los fines del procesamiento de dichos datos y de las personas u organizaciones con las que se comparten. Los sistemas de reconocimiento facial también pueden tener sesgos tecnológicos inherentes, por ejemplo, cuando se basan en color de piel u origen étnico.

La “privacidad desde el diseño” puede ayudar a abordar los riesgos

La privacidad desde el diseño busca ofrecer el máximo grado de privacidad, garantizando que las protecciones de datos personales estén integradas en el sistema de forma predeterminada. La privacidad desde el diseño puede, por ejemplo, implicar el uso de datos agregados, anónimos o seudónimos para



proporcionar protección adicional, así como la eliminación de datos una vez que se cumpla el propósito para el cual fueron recolectados.

Por ejemplo, la aplicación para el COVID-19 desarrollada por el Instituto Noruego de Salud Pública está diseñada para almacenar datos de ubicación sólo durante 30 días. El uso de soluciones adicionales para mejorar la privacidad (como el cifrado homomórfico)¹ puede proporcionar mayor seguridad, al igual que el uso de espacios aislados de datos, a través de los cuales el acceso a datos altamente sensibles (personales) sólo se concede dentro de un entorno digital y/o físico restringido a usuarios de confianza. Un ejemplo de esto último es Flowminder, que colaboró con las empresas de telecomunicaciones durante el brote de ébola de 2014-16 para proporcionar a los epidemiólogos acceso seguro a datos de geolocalización anonimizados y de baja resolución. Flowminder está utilizando una estrategia similar para contribuir a la respuesta a la crisis del COVID-19.

Recomendaciones clave

Las tecnologías digitales proporcionan herramientas poderosas a los gobiernos en su lucha para controlar la pandemia del COVID-19, pero sus alcances en términos de privacidad y protección de datos deben ser identificados. Las aplicaciones de seguimiento de contactos deben implementarse con total transparencia, en consulta con las principales partes interesadas, incluyendo protecciones de privacidad sólidas desde el diseño y, cuando corresponda, ser desarrolladas a través de proyectos de código abierto. Los gobiernos deberían considerar:

- La base jurídica para el uso de estas tecnologías, que varía según el tipo de datos recopilados (por ejemplo: personales, sensibles, “pseudonimizados”, anonimizados, agregados, estructurados o no estructurados).
- Si el uso de estas tecnologías y su recopilación de datos es proporcional, y cómo se almacenan, procesan, comparten y con quién (incluyendo qué protocolos de seguridad y privacidad por diseño se implementan).
- La calidad de los datos recogidos y si son aptos para su propósito.
- Si el público está bien informado y si los enfoques adoptados se aplican con total transparencia y responsabilidad.
- El período de tiempo dentro del cual las tecnologías más invasivas de recopilación de datos personales pueden utilizarse para enfrentar la crisis. Los datos deben conservarse únicamente durante el tiempo que sea necesario para cumplir el propósito específico para el que fueron recopilados.

Lectura complementaria

OCDE (2019a), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, París, <https://doi.org/10.1787/276aaca8-en>.

OCDE (2019b), *Recommendation of the Council on Artificial Intelligence*, OCDE, París, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

OCDE (2017), *Recommendation of the Council on Health Data Governance*, OCDE, París, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433>.

OCDE (2015), “Mobile technology-based services for global health and wellness: Opportunities and challenges”, página web, OCDE, París, www.oecd.org/sti/ieconomy/mobile-technology-based-services-for-global-health.htm.

¹ Permite el procesamiento de datos cifrados sin necesidad de revelar la información subyacente.



La OCDE está recopilando datos, análisis y recomendaciones sobre los desafíos sanitarios, económicos, financieros y sociales que plantea el impacto del coronavirus (COVID-19).

Visite nuestra [página dedicada](#) para obtener más información relacionada con el coronavirus.

Publicado originalmente por la OCDE bajo el título: OCDE (2020), Tracking and Tracing Covid: Protecting privacy and data while using apps and biometrics, https://read.oecd-ilibrary.org/view/?ref=129_129655-7db0lu7dto&title=Tracking-and-Tracing-COVID-Protecting-privacy-and-data-while-using. Traducido con el apoyo de la Delegación Permanente de Colombia ante la OCDE. Esta no es una traducción oficial de la OCDE. En caso de discrepancia entre el documento original y la traducción, sólo se considerará válido el texto del documento original.

El presente trabajo se publica bajo la responsabilidad del Secretario General de la OCDE. Las opiniones expresadas y los argumentos utilizados en el mismo no reflejan necesariamente el punto de vista oficial de los países miembros de la OCDE.

Tanto este documento, como cualquier dato y cualquier mapa que se incluya en él, se entenderán sin perjuicio alguno respecto al estatus o la soberanía de cualquier territorio, a la delimitación de fronteras y límites internacionales, ni al nombre de cualquier territorio, ciudad o área.

El uso de este trabajo, ya sea en su versión digital o impresa, se rige por los términos y condiciones que se encuentran en <http://www.oecd.org/termsandconditions>

