Garantizar la privacidad de datos mientras luchamos contra el COVID-19

14 abril 2020

Mensajes clave

- Muchos gobiernos están tomando medidas nunca antes vistas para detectar, rastrear y contener la propagación del nuevo coronavirus (COVID-19), al recurrir a las tecnologías digitales y a la analítica avanzada para recabar, procesar y compartir datos a fin de ofrecer primeras líneas de respuesta eficaces.
- Aunque es posible que las medidas excepcionales implementadas o previstas por algunos países sean eficaces en última instancia para limitar la propagación del virus, algunas tácticas han generado polémica debido a los riesgos que presentan para la privacidad y otros derechos fundamentales de los ciudadanos, sobre todo cuando esas medidas carecen de transparencia y consulta pública.
- En general, las autoridades encargadas de proteger la privacidad de los ciudadanos han adoptado un enfoque pragmático y contextual en tiempos de crisis o de emergencia, y han ejercido su criterio para hacer cumplir la ley, recordando que el respeto a los principios fundamentales de privacidad y protección de datos no obstaculiza la implementación de respuestas de primera línea necesarias y proporcionales para combatir el COVID-19.
- Tras consultar con las autoridades competentes en materia de privacidad, los responsables de la formulación de políticas públicas deben evaluar las posibles ventajas e inconvenientes de utilizar los datos durante esta crisis, conciliando riesgos y beneficios; así mismo, deben garantizar que toda medida extraordinaria sea proporcional a los riesgos y se implemente con total transparencia, rendición de cuentas y el compromiso de suspender o revocar de inmediato el uso excepcional de datos cuando la crisis haya terminado.

Algunas respuestas digitales a la crisis han provocado nuevos desafíos para la privacidad y la gobernanza de datos

Los gobiernos están tomando medidas nunca antes vistas para rastrear y contener la propagación del nuevo coronavirus (COVID-19), y están aprovechando el poder de los datos para impulsar soluciones digitales. De particular importancia para una primera línea de respuesta eficaz es la información sobre la propagación del virus, como la ubicación y el número de nuevos casos confirmados, las tasas de recuperación y de mortalidad, y el origen de nuevos casos (llegadas internacionales o transmisión comunitaria). Los datos también son fundamentales para calcular y mejorar la capacidad de los sistemas de la salud y para evaluar la eficacia de las políticas de contención y mitigación que limitan la circulación de las personas. Muchos gobiernos están recurriendo a las tecnologías digitales y a la analítica avanzada para recabar, analizar y compartir datos para las primeras líneas de respuesta, en particular: (i) datos de ubicación geográfica derivados del registro de datos de llamadas móviles de los usuarios o recopilados por aplicaciones móviles; y (ii) biometría, principalmente datos de reconocimiento facial.

Por lo tanto, el acceso e intercambio oportuno, seguro y confiable de datos es decisivo para entender al virus y su propagación, lo que mejora la eficacia de las políticas gubernamentales y fomenta la cooperación mundial en la carrera para desarrollar y distribuir tratamientos y vacunas.

Pero algunas respuestas a la crisis están creando nuevos desafíos para la privacidad y la gobernanza de datos. Por ejemplo, si bien las tecnologías de rastreo de contactos pueden ser útiles al proporcionar información crucial para limitar la propagación del virus, también pueden utilizarse para una recopilación e intercambio exhaustivo de datos personales si no se controlan, lo cual puede derivar en una vigilancia colectiva que limitaría las libertades individuales y pondría en entredicho la gobernanza democrática.

Pocos países cuentan con sistemas que apoyen las medidas extraordinarias de rastreo de contactos y vigilancia demográfica previstas

Las medidas previstas en algunos países ya han generado polémica por los riesgos que presentan para la privacidad y otros derechos fundamentales de los ciudadanos, en particular cuando esas medidas carecen de transparencia y consulta pública. Incluso si los datos personales son de carácter anónimo, investigaciones recientes sugieren que es posible identificar a personas aún con un conjunto limitado de datos: cuatro puntos espacio-temporales pueden bastar para identificar de manera inconfundible al 95% de las personas en una base de datos de teléfonos celulares de 1,5 millones de usuarios, e identificar al 90% de las personas en una base de datos de tarjetas de crédito de 1 millón de usuarios.

Pocos países cuentan con sistemas para apoyar estas medidas extraordinarias de forma rápida, segura, confiable, escalable y en cumplimiento con las normas vigentes de privacidad y protección de datos. Por lo tanto, en los últimos meses, muchos países aprobaron —o están a punto de aprobar — leyes que especifican cómo la recopilación de datos se limitará a una determinada población, durante cuánto tiempo y con qué propósito. Por ejemplo:

- El gobierno italiano publicó un Decreto que establece un marco legal especial para que, durante el estado de emergencia, las autoridades de salud pública y las empresas privadas que forman parte del sistema sanitario nacional recaben y compartan datos personales relacionados a la salud.
- El gobierno alemán propuso enmendar la Ley de Protección contra Enfermedades Infecciosas para permitir que el Ministerio Federal de Salud solicite a las personas “en riesgo” que se identifiquen y proporcionen información sobre su historial de desplazamientos, así como datos sobre las personas con quienes tuvieron contacto. La propuesta original, que otorgaba poderes más amplios para utilizar medios técnicos a fin de identificar a personas potencialmente

contagiadas y obtener datos de ubicación geográfica a través de los proveedores de telecomunicaciones, se ha retirado en forma parcial debido a las fuertes críticas del Comisionado Federal de Protección de la Privacidad.

- Al analizar el proyecto de ley de emergencia, los senadores franceses propusieron una enmienda que permitiera, durante un lapso de seis meses, "cualquier medida" que posibilitara la recopilación y procesamiento de datos de ubicación y salud para hacer frente a la epidemia del COVID-19. La enmienda fue rechazada por ser una fuerte intrusión a los derechos a la privacidad.

Algunos gobiernos han recopilado y procesado datos de ubicación geográfica relacionados con el COVID-19 sin necesidad de aprobar una nueva legislación. Cabe mencionar los siguientes ejemplos:

- Las autoridades de la República de Corea ya tienen poderes extraordinarios para recabar datos personales si es "necesario para prevenir enfermedades contagiosas e impedir que se propague la infección" (Ley sobre la Prevención y Control de Enfermedades Contagiosas, Artículo 76-2).
- En Singapur, se pueden recopilar, utilizar y divulgar datos personales pertinentes durante un brote sin consentimiento del ciudadano para efectuar el rastreo de contactos y tomar medidas de respuesta.
- En Israel, el gobierno ha dictado medidas de emergencia que permiten utilizar la tecnología creada para combatir al terrorismo a fin de rastrear a las personas contagiadas a través del monitoreo de teléfonos móviles.

Las autoridades de protección de la privacidad desempeñan un papel fundamental cuando los gobiernos promulgan leyes de emergencia y los controladores de datos buscan seguridad jurídica

Pese a la magnitud de los problemas económicos y de salud pública planteados por la pandemia del COVID-19, es crucial que los gobiernos y las instancias del sector privado no se alejen de los principios fundamentales sobre la privacidad y la gobernanza de datos. Las autoridades de protección de la privacidad (APP) desempeñan un papel fundamental al asesorar sobre nuevas propuestas legislativas y dar claridad sobre la correcta aplicación de las normativas existentes en materia de privacidad y protección de datos. Es posible que las APP necesiten ofrecer soluciones innovadoras y progresistas, sobre todo cuando se trata de asuntos importantes como eliminar o conservar datos personales, la reversibilidad de los nuevos controles gubernamentales y el ejercicio de sus poderes de auditoría e investigación.

A mediados de abril de 2020, las APP en Argentina, Australia, Canadá, Finlandia, Francia, Alemania, Irlanda, Nueva Zelanda, Polonia, Eslovaquia, Suiza y el Reino Unido publicaron lineamientos generales para controladores y procesadores de datos sobre la aplicación de las leyes de protección de datos y privacidad durante la crisis. En general, las autoridades que aplican las leyes de protección de la privacidad han respaldado un enfoque pragmático y contextual, y han ejercido su criterio en cuanto al cumplimiento de la ley, recordando que el respeto a los principios fundamentales de la privacidad y protección de datos no obstaculiza la implementación de respuestas de primera línea necesarias y proporcionales para combatir el COVID-19. El Comité Europeo de Protección de Datos y el Consejo de Europa han publicado declaraciones similares, explicando que el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) y el Convenio 108 no entorpecen las medidas tomadas para luchar contra la pandemia, pero sí exigen que, en un periodo de emergencia, las restricciones a las libertades sean proporcionales y se limiten a dicho periodo.

Algunas APP han publicado lineamientos específicos, como por ejemplo las reglas que se deben aplicar en el uso de información de redes sociales para rastrear a posibles portadores (p.ej., Hong Kong, China) y las acciones que debería tomar el gobierno con respecto a las crecientes estafas y el surgimiento de "productos milagro" para tratar el virus o prevenirlo (como en España y Estados Unidos).

En otros casos, las APP están respondiendo en formas innovadoras. Por ejemplo, la Oficina del Comisionado de Información del Reino Unido anunció que reconocerá el carácter de urgente que la aplicación de la ley de protección de datos tiene en el interés público y permitirá que los controladores de datos equilibren sus obligaciones con su capacidad para responder a las solicitudes de acceso. Global Privacy Assembly, un consorcio mundial de órganos reguladores de la privacidad y la protección de datos, creó una página de recursos especiales que recopila los lineamientos generales y la información más reciente proporcionada por sus miembros.

Recomendaciones clave

Las respuestas de política pública están evolucionando con rapidez en un entorno caracterizado por una disponibilidad limitada de evidencia y poca oportunidad de efectuar consultas internas o multilaterales sólidas. Sin embargo, todos los países necesitan datos de manera apremiante para informar las respuestas normativas y de política pública conforme evoluciona la crisis. Las siguientes reflexiones, que se basan en los principios de la OCDE sobre la privacidad y gobernanza de datos, deberían guiar las prácticas de recopilación e intercambio de datos de los países.

- **Los gobiernos necesitan promover el uso responsable de los datos personales.** Al parecer, existe una tendencia creciente para recopilar, procesar e intercambiar datos conductuales y de salud personales a gran escala de manera más invasiva, lo cual implica una vigilancia focalizada de personas para contener la propagación del COVID-19. Si bien algunas de estas medidas pueden ser eficaces para ayudar a contener el brote, los gobiernos deberían garantizar que esas herramientas se implementen con total transparencia, rendición de cuentas y con el compromiso de suspender o revocar rápidamente los usos excepcionales de datos cuando la crisis haya terminado. Los controladores de datos deben seguir teniendo un fundamento legal y válido para recopilar y utilizar datos personales.
- **Los gobiernos deberían consultar a las APP *antes* de introducir medidas cuya implementación pueda infringir los principios de privacidad y protección de datos.** Debería consultarse a las APP sobre los esfuerzos de primera línea para asegurar que las intromisiones a los derechos a la privacidad incluyan las garantías adecuadas. Las autoridades de protección de la privacidad y los gobiernos deben poner recursos expertos a disposición para posibilitar esas evaluaciones.
- **Las APP deben abordar las incertidumbres en materia de regulación.** Deben adoptar un enfoque contextual y pragmático para responder con rapidez a las peticiones de asesoría y aclarar, para cada jurisdicción, cómo se debe aplicar la normativa de privacidad y protección de datos a la recopilación y el intercambio de datos personales durante esta crisis. Es probable que al hacerlo se fomente el cumplimiento de esas normativas y se faciliten flujos de datos internos y transfronterizos más eficientes.
- **Conforme a las garantías proporcionales y necesarias, los gobiernos deben apoyar la cooperación nacional e internacional para recabar, procesar e intercambiar datos de salud personales para la investigación, estadística y otros fines relacionados con la salud pública al gestionar la crisis del COVID-19.** Esto incluye adoptar soluciones para el acceso e intercambio de datos que protejan la privacidad y, cuando sea oportuno, participar en asociaciones público-privadas para facilitar el intercambio de datos.
- **Los gobiernos y los controladores de datos deben ser transparentes y rendir cuentas de todas las medidas que tomen en respuesta a la crisis.** Los gobiernos deben asegurar la participación, principalmente a través de la consulta pública, de todos los sectores de la sociedad con el propósito de garantizar que la recopilación, procesamiento e intercambio de datos

personales sirvan al interés público y sean compatibles con los valores sociales y las expectativas razonables de las personas.

Lectura complementaria

OECD (2020), *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics,* OECD, Paris, https://read.oecd-ilibrary.org/view/?ref=129_129655-7db0lu7dto&title=Tracking-and-Tracing-COVID-Protecting-privacy-and-data-while-using

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

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

OECD (2013), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.