



Guía

Para el tratamiento de los datos personales en el uso de herramientas de geolocalización

La Ley 25.326 de Protección de Datos Personales y el Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, aprobado en nuestro país por la Ley 27.483, no prohíben el monitoreo de la ubicación de las personas, pero las medidas de tratamiento de datos que se implementen deben realizarse respetando el derecho humano a la privacidad de las personas.

A continuación, la Agencia de Acceso a la Información Pública señala los principios fundamentales de la regulación vigente en materia de protección de datos que se aplican al uso de herramientas de geolocalización y tracking, ya sea que dichas herramientas sean empleadas por el sector público, el sector privado o por ambos en colaboración:

1

Toda información referida a la ubicación de una persona y/o sus desplazamientos constituye un dato personal, protegido bajo la Ley 25.326. A efectos de recoger y tratar ulteriormente esta categoría de información, es necesario que el responsable se ampare en alguna de las bases legales contempladas en el Artículo 5 de la Ley 25.326. La recopilación de datos de ubicación podrá realizarse cuando:

- El titular de los datos haya prestado su consentimiento libre, expreso e informado. El consentimiento podrá ser obtenido a través de la aceptación de términos y condiciones en una aplicación o plataforma web.
- Los datos se obtengan de fuentes de acceso público irrestricto.
- Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

- Deriven de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento.

2

Los datos de ubicación son definidos como información recopilada por una red o servicio sobre dónde está o estaba ubicado el teléfono del usuario u otro dispositivo. Por ejemplo, sería posible rastrear la ubicación de un teléfono móvil a partir de los datos recopilados por las estaciones base en una red de telefonía móvil.

3

Los datos de ubicación pueden inferirse por GPS (sistema de posicionamiento global), torres de celdas (operadores de telefonía móvil), redes wifi, bluetooth o una combinación de señales.

4

Estos datos pueden estar en poder de:

- Proveedores de servicios de telecomunicaciones (prestan servicio central para tener conexión).
- Proveedores de servicios de Internet.
- Servicios de valor agregado, tales como aplicaciones bajadas por el usuario, quien presta su consentimiento sobre el procesamiento de datos de tráfico o datos de ubicación.

5

Los organismos estatales estarán autorizados a realizar el monitoreo siempre y cuando lo hagan en el ámbito de su competencia específica. Dicha competencia deberá ser interpretada en sentido estricto y no amplio. Cuando no cuenten con esta autorización, el monitoreo deberá ampararse en otra base legal alternativa, tal como el consentimiento.

6

Para la cesión de datos referidos a la ubicación de una persona y/o sus desplazamientos entre organismos públicos, no se requiere el consentimiento del titular de los datos en la medida en que el cedente haya obtenido los datos en ejercicio de sus funciones, el cesionario utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de su competencia y, por último, los datos involucrados sean adecuados y no excedan el límite de lo necesario en relación a esta última finalidad (Criterio 5 de la [Resolución AAIP 4/2019](#)).

7

Los responsables de tratamiento de datos personales pueden realizar actividades de monitoreo si los datos se encuentran disociados, en cuyo caso no resulta aplicable la Ley 25.326 porque el dato disociado no es un dato personal. El dato

de ubicación será considerado disociado cuando el procedimiento que deba aplicarse para lograr su identificación con una persona requiera la aplicación de medidas o plazos desproporcionados o inviables (Criterio 3 de la [Resolución AAIP 4/2019](#)).

8

Cuando el monitoreo esté autorizado por el consentimiento del titular de los datos, el responsable de tratamiento de datos personales debe darle al titular la oportunidad de revocarlo en cualquier momento.

9

Para monitorear o seguir la geolocalización de una persona, los responsables de tratamiento de datos personales deben respetar en todo momento el principio de calidad del dato, previsto en el Artículo 4 de la Ley 25.326. Ello implica que:

- Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. En el caso concreto del monitoreo o el seguimiento de geolocalización, este debe limitarse a finalidades asociadas a paliar los efectos del coronavirus COVID-19 y no debe interferir arbitrariamente en la privacidad de la persona que es objeto del monitoreo.
- La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la Ley 25.326. El monitoreo debe hacerse al descubierto, informando a la población.
- Los datos objeto de monitoreo no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. El monitoreo no puede ser extendido a otras finalidades que no se relacionen con mitigar los efectos del coronavirus COVID-19.
- Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. Es indispensable que la herramienta sea precisa y que no dé lugar a errores que puedan generar un efecto negativo o perjudicar un derecho del titular de los datos.
- Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate.
- Los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación y supresión de datos personales contemplados en los Artículos 14 y 16 de la Ley 25.326.

- Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. Cuando el monitoreo haya sido revocado por el titular de datos o cuando su finalidad haya sido cumplida, por ejemplo, porque la pandemia del coronavirus COVID-19 llegó a su conclusión, los datos deben eliminarse. El almacenamiento debe permitir que los datos personales sean identificables para facilitar su posterior eliminación.

10

El responsable debe cumplir, además, con el principio de información previsto en el Artículo 6 de la Ley 25.326. Ello significa que debe aclarar cómo y por qué realiza el seguimiento de personas, en dónde se almacena la información, con quiénes se comparten esos datos, las consecuencias del tratamiento y la posibilidad que tiene el titular de los datos de ejercer los derechos de acceso, rectificación o supresión.

11

Asimismo, los datos deben ser almacenados de modo que se cumplan los principios de seguridad y confidencialidad previstos en los Artículos 9 y 10 de la Ley 25.326. A esos efectos, se recomienda adoptar las medidas de seguridad recomendadas en la [Resolución AAIP 47/2018](#).

12

Teniendo en cuenta que el monitoreo de la ubicación y/o los desplazamientos de una persona tiene el potencial de afectar tanto la privacidad como otros derechos de los titulares de datos, se recomienda al responsable de tratamiento de datos personales realizar una evaluación de impacto de manera previa a la implementación de la herramienta, con el fin de controlar y mitigar sus riesgos, así como evaluar su viabilidad. Dicha evaluación de impacto podrá realizarse conforme a la [Guía de Evaluación de Impacto en la Protección de Datos](#) elaborada por la Agencia en colaboración con la Unidad Reguladora y de Control de Datos Personales de la República Oriental del Uruguay.

