¿Por qué se debe modificar el Decreto Legislativo 1182?

El **Decreto Legislativo No. 1182** es una norma publicada el 27 de julio de 2015 por el Poder Ejecutivo en el marco de las facultades legislativas que el Congreso le otorgó en materia de seguridad ciudadana. Este Decreto autoriza a la policía conocer la ubicación de cualquier usuario de celulares sin necesidad de orden judicial y ordena a las empresas operadoras a conservar los registros de todas las comunicaciones fijas, móviles y por Internet de los peruanos por hasta tres años para ser consultados por el Estado. Aunque otorgar mejores herramientas al Estado para combatir la delincuencia es una necesidad de especial interés, ello no puede suponer la afectación desproporcionada de los derechos fundamentales. La publicación de esta norma y los potenciales riesgos que implica para la privacidad de todos los peruanos ha sido destacada por medios nacionales e internacionales como New York Times, The Guardian, Slate, entre otros.

La ***información de geolocalización*** es producida por todos los celulares (*smartphones* o no) y *tablets* conectados a una red pública de comunicaciones y se genera automáticamente sin que el usuario se de cuenta. De acuerdo con la nueva norma, la Policía podrá conocer la última ubicación y seguir en tiempo real el desplazamiento de cualquier usuario de estos dispositivos con solo solicitarlo a las empresas operadoras. Para ello, bastará que a su solo criterio determinen que: existe flagrancia delictiva, se trata de un delito penado con más de cuatro años de cárcel y dicha información es necesaria para la investigación. En paralelo, deberán de poner estos hechos en conocimiento de un Fiscal, quien deberá de solicitarlo a un Juez, el que a su vez podrá confirmar o desautorizar la medida. Mientras que la Policía obtendrá acceso inmediato a la geolocalización de un usuario, pasarán al menos 72 horas para que la legalidad de dicho acceso pueda ser evaluada. Este nuevo sistema va en contra de la Constitución y sus normas de desarrollo, que han señalado que los datos de geolocalización están protegidos por el secreto de las telecomunicaciones y, por tanto, solo puede accederse a ellos mediante el mandato previo y motivado de un juez. Las circunstancias habilitantes que señala la norma son demasiado vagas y no pueden ser fácilmente evaluadas por un policía. El mecanismo de revisión judicial posterior no garantiza que este sistema no pueda ser incorrectamente utilizado. Además, ya existe un mecanismo en el Código Procesal Penal para que el Ministerio Público pueda acceder a esta información mediante autorización judicial (artículo 230).

Por otro lado, la norma también dispone la ***conservación de la información derivada de las telecomunicaciones*** de todos los peruanos por tres años por las empresas operadoras. Esta información incluye registro de llamadas, duración, frecuencia, registro de geolocalización, tipo de contenidos visitados en Internet, números IPs, entre otros. La finalidad de esta medida es crear una base de datos masiva que el Estado pueda utilizar en eventuales investigaciones criminales bajo orden judicial. En la práctica, equivale a que se ordene registrar y monitorear a todos los peruanos inocentes o culpables, menores o mayores de edad, incluyendo periodistas, políticos o dirigentes sociales "por si acaso" cometan algún delito. La práctica de retención o conservación de datos masiva ha sido declarada inválida el año pasado por el Tribunal de Justicia de la Unión Europea y ha sido condenada por el Relator Especial para la Libertad de Expresión de Naciones Unidas por afectar desproporcionada e innecesariamente la privacidad de los ciudadanos. La creación de una base de datos de este tipo constituye en sí misma una afectación a la privacidad y su manipulación genera un riesgo desproporcionado para todos.

Pese a lo controvertido de estas nuevas medidas, el Poder Ejecutivo no ha sustentado ni técnica ni jurídicamente sus propuestas. Aunque señalan que el marco legal anterior no dejaba a la Policía hacer su trabajo, no se señalan estadísticas sobre el número de solicitudes procesadas para acceder a datos personales, el tiempo que el Poder Judicial ha demorado en aceptarlas o las veces en que han servido o no para combatir la delincuencia. Por el contrario, párrafos enteros de la Exposición de Motivos han sido plagiados de un ensayo colombiano escrito precisamente en contra de la conservación de datos que concluye que dicha práctica es inconstitucional.

¿Cómo se puede mejorar?

Exigiendo que todo acceso por parte de la Policía Nacional o el Ministerio Público a los datos de geolocalización de cualquier usuario de dispositivos móviles sea autorizado y motivado por un juez. Para ello, pueden establecerse plazos de respuesta judicial menores a 24 horas a través de jueces de turno o juzgados especiales. En el caso de la conservación de datos, esta medida solo debería de ser ordenada por juez respecto de uno o varios usuarios de servicios públicos de telecomunicaciones en particular y por un período de tiempo proporcional a los fines de la investigación.

¿Qué puede hacer el Congreso?

Según la Constitución y el Reglamento del Congreso, la Comisión de Constitución tiene el deber de emitir un dictamen sobre la legalidad de las propuestas dentro de los siguientes diez (10) días hábiles de recibido el Decreto Legislativo. Adicionalmente, cualquier otro congresista puede promover una reforma legislativa independiente para corregir los puntos críticos del Decreto Legislativo. Complementariamente, deben de existir reglas específicas sobre la conservación, uso y eventual destrucción de la información a la que se acceda a través de estos mecanismos así como obligaciones de reportar periódicamente estadísticas sobre su uso y efectividad.

Sobre Hiperderecho

Hiperderecho es una asociación civil sin fines de lucro formada en el 2012 dedicada a investigar y promover el respeto de los derechos humanos en entornos digitales, conformada por abogados y especialistas en tecnología. Como parte de nuestro trabajo, estudiamos todas las propuestas legislativas que están relacionados con el ejercicio de los derechos a la libertad de expresión, la privacidad y el ejercicio de los mismos en entornos digitales.

> «De ese modo, el derecho a la vida privada tutela a las conversaciones telefónicas independientemente de su contenido e incluso puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones.»
>
> **Corte Interamericana de Derechos Humanos, *Caso Escher y otros vs. Brasil* (2009)**

> «La preocupación sobre si el acceso a los datos y su uso se ajustan a objetivos legítimos específicos plantea también dudas sobre la creciente colaboración de los gobiernos con entidades del sector privado para que conserven datos "por si acaso" los necesita el gobierno. La conservación obligatoria de datos de terceros —característica frecuente de los regímenes de vigilancia de muchos Estados, cuyos gobiernos exigen a las compañías telefónicas y a los proveedores de servicios de Internet que almacenen los metadatos acerca de las comunicaciones y la ubicación de sus clientes para que las fuerzas del orden y los organismos de inteligencia puedan acceder posteriormente a ellos— no parece necesaria ni proporcionada.»
>
> **Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *El Derecho a la Privacidad en la Era Digital*, A/HRC/27/37**

Para conocer más sobre esta norma, los cuestionamientos planteados y las reformas posibles puede comunicarse con Miguel Morachimo, Director de Hiperderecho, escribiendo a miguel@hiperderecho.org