El Derecho Fundamental a la Protección de Datos Personales

La Autoridad Nacional de Protección de Datos Personales APDP

PERU

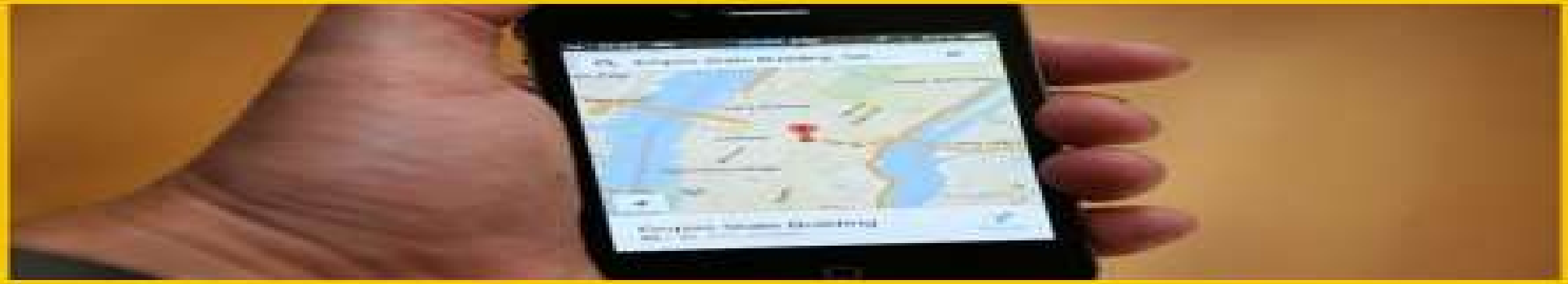
Ministerio de Justicia y Derechos Humanos

José Alvaro Quiroga León

Director General

Debate: ¿La ley de geolocalización es legítima?

A favor y en contra. José Álvaro Quiroga explica por qué cree que sí. Por su parte, Dino Caro Coria argumenta por qué no.



Ley 'stalker': Defensoría realizó recomendaciones a la norma

Ley 'stalker': Mininus dice que cuenta con apoyo de operadores

Pérez Guadalupe: Se han creado "fantasmas" sobre Ley 'stalker'

¿Norma para que policía localice móviles viola la privacidad?

Pérez Guadalupe: "Nadie quiere volver a la época de Montesinos"

¿Sin orden judicial?

- DINO CARO CORIA -
Abogado

Desde hace dos años existe la geolocalización en el Perú. Este mecanismo no es nuevo, y busca luchar contra la criminalidad. Desde el 2013, el artículo 230 inciso 4 del Código Procesal Penal (CPP) obliga a las empresas de telecomunicaciones a entregar a la policía dicha información siempre "que haya sido dispuesta mediante resolución judicial". De ese modo, la policía debe primero obtener la autorización de un juez.

Así, lo único nuevo del reciente Decreto Legislativo 1182 es que la policía podrá obtener la ubicación de las personas sin una orden judicial previa. Es decir, de manera inmediata y directa sin mayores 'trámites burocráticos'. Sin embargo, a pesar de que el gobierno ha puesto de relieve los candados de la ley, esto no genera absoluta seguridad en el manejo de la información y el respeto de los derechos individuales, en especial la intimidad. Ahora la policía accederá a la geolocalización en los casos que considere de necesidad, cuando el flagrante delito tenga una pena mínima de 4 años de prisión. Asimismo, existirá un control judicial posterior, en el que el fiscal debe pedir al juez la convalidación de la medida.

Como la nueva ley no ha derogado el artículo 230 del CPP, ambas han quedado subsistentes. Por un lado, el CPP solo regiría cuando no exista flagrancia o para delitos con penas inferiores a 4 años. Por otro, con la promulgación del decreto, la geolocalización se ha convertido en un método policíaco de investigación directa y a la mano de la policía. Esto es peligroso debido a la existencia de un mercado negro de 'chuponeos' e interceptaciones ilegales. Además, es absolutamente inconstitucional como lo demuestra el artículo 2 inciso 10 de la Constitución: "Las [...] telecomunicaciones o sus instrumentos solo pueden ser [...] interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley". Y es que la geolocalización de un celular, una laptop o una tableta solo es posible mediante la intervención de los equipos y de la línea o red que los conecta, lo que implica a la vez una injerencia contra la intimidad personal, ya que la policía podrá conocer en tiempo real todos los lugares en donde nos encontremos.

Por ello, la exigencia de una orden judicial previa para el acceso a la geolocalización no puede verse como una traba burocrática, sino como la irrenunciable garantía ciudadana de que en una democracia el acceso a la intimidad personal no puede depender de una decisión administrativa o policíaca. En ese sentido, se trata de una medida cautelar. El Estado con esta ley busca afectar los derechos fundamentales. Por eso, los criterios de necesidad, ponderación, flagrancia o pena superior a 4 años demandan una especial valoración jurídica, ajena e imparcial que en un Estado de derecho compete solo a los jueces.

La eficacia policial demanda que los jueces actúen con celeridad, pero de ello no se deduce que debamos renunciar al control judicial, sino acelerarlo. En ese camino, la mejor alternativa es facultar a los jueces de turno, como sucede en Estados Unidos y en Europa, a que puedan resolver las peticiones de geolocalización en tiempo real incluso por teléfono. Todo ello, cuando el caso así lo demande y cuando la injerencia a la intimidad personal esté justificada.

Antidelincuentes

- JOSÉ ÁLVARO QUIROGA -
Director general de Protección de Datos Personales del Ministerio de Justicia

Al comentar el Decreto Legislativo 1182, sobre acceso a datos de telecomunicaciones para la lucha contra la delincuencia, se ha seguido la tradición nacional de atribuirle a la norma un contenido que no tiene. Por ejemplo, que se autoriza el acceso al contenido de las comunicaciones de los ciudadanos y que quien accede es el gobierno. Sin embargo, quien lea la norma verá que las críticas de este tipo se descalifican solas y no vale la pena dedicarles más tinta.

Asimismo, existen los que se basan en pronosticar probables "malos usos" por parte de la policía. Bajo ese supuesto, la futurología ligera nos llevaría a prohibir la circulación de patrulleros porque podrían usarse para atropellar. Como si esa fuera la finalidad de las herramientas destinadas a combatir la delincuencia. En este terreno cualquier especulación sirve para llevarnos al absurdo.

Es curioso que quienes critican el acceso de la policía a la ubicación de delincuentes como un pecado contra la privacidad sean los mismos que defienden el comercio de datos personales de cualquier peruano y sostienen que impedirlo afecta la transparencia.

Por otro lado, se alude a la protección constitucional de las comunicaciones y a decisiones extranjeras sobre conservación y acceso a información de telecomunicaciones. En efecto, son opiniones más serias, sobre las que sí vale la pena detenerse para advertir que se refieren a escenarios similares pero con ciertas diferencias y ahí está el detalle.

Analicemos el siguiente supuesto: un ciudadano identificado es objeto de acceso ilegítimo (porque también hay legítimo) a "sus comunicaciones" y en ese contexto es tan ilegítimo conocer el contenido como el récord de sus comunicaciones (con quién, con qué frecuencia e incluso desde dónde se comunica). Este es un escenario en el que no cabe duda de que la geolocalización vulnera la privacidad constitucionalmente protegida de esa persona.

Otro caso es que la información general de comunicaciones de todos los ciudadanos es objeto de un mandato legal de conservación. Ello se pone a disposición para acceso indiscriminado de la policía para que busquen información. Este es el escenario del cual viene regresando Europa, por ejemplo, después de que los ataques terroristas generaron respuestas que se consideraron constitucionalmente insostenibles por ser "desproporcionadas". Eso no quiere decir que hoy la información no sea accesible en el marco de una investigación concreta, es decir "proporcional".

El escenario en el que se aplica el Decreto Legislativo 1182 es otro: un dispositivo, móvil o no, se acaba de usar para consumar una extorsión bajo amenaza o secuestro. Entonces, la policía requiere acceder a la información de ubicación o titularidad del dispositivo para detener el crimen. Usar el derecho de la privacidad para proteger los datos de los delincuentes resulta, más que una paradoja, un sinsentido. Además, implica saber que la delincuencia se sirve de la tecnología, mientras que nuestra sociedad, ingenuamente, le niega a la policía la posibilidad de acceder a la información.

Finalmente, la Ley 29924, que sanciona las llamadas malintencionadas a centrales de emergencias, ha establecido que la identificación de estas llamadas no constituye una vulneración del derecho al secreto de las telecomunicaciones. Entonces, ¿por qué no se cuestionó esta disposición, que sirve para combatir una infracción administrativa, como se hace ahora contra aquella que sirve para combatir delitos graves?

Se trata de una norma sobre acceso a datos de telecomunicaciones para la lucha contra la delincuencia.

Que se comento sobre el Decreto Legislativo 1182?

Primer paso: se atribuye a la norma un contenido que no tiene.

- Que autoriza acceso al contenido de las comunicaciones.
- Que puede afectar a cualquier ciudadano.
- Que quien accede es “el gobierno”.

Segundo paso: se pronostican “malos usos” por parte de la policía.

- Nos llevaría a prohibir la circulación de patrulleros porque podrían usarse para atropellar.
- Nos llevaría a quitarles las armas porque pueden usarse para robar,
- No se aprecia la finalidad normal de las herramientas destinadas a combatir la delincuencia.

La libre especulación nos lleva al absurdo.

Dato curioso:

Quienes critican el acceso de la policía a la ubicación de delincuentes,como un pecado contra la privacidad, son los mismos que usualmente defienden el comercio de datos personales de cualquier peruano como ejercicio de “transparencia”

Una perspectiva enfocada desde la PDP

Efectivamente, la protección constitucional de las comunicaciones ha afectado decisiones sobre conservación y acceso a información de telecomunicaciones

En PDP sabemos que pueden presentarse escenarios similares, cuyas diferencias y matices marcan:

- La legitimidad de las finalidades
- La proporcionalidad de los tratamientos

Escenarios diversos

- Un ciudadano identificado es objeto de acceso ilegítimo (porque también hay legítimos) a “sus comunicaciones”

Es tan ilegítimo conocer el contenido como el récord de sus comunicaciones (con quién, con qué frecuencia e incluso desde dónde se comunica). Y en este escenario la geolocalización forma parte la privacidad constitucionalmente protegida de esa persona.

- La información general de comunicaciones de todos los ciudadanos es objeto de un mandato de conservación y puesta a disposición para acceso indiscriminado de la policía para “buscar” o “pescar” información.

Este es el escenario del que regresa Europa, después de medidas que se han considerado constitucionalmente insostenibles por “desproporcionadas”.

No quiere decir que hoy la información no sea accesible, en el marco de una investigación concreta, es decir “proporcional”.

- Un dispositivo, móvil o no, se acaba de usar para consumar una extorsión y la policía requiere acceder a la información de ubicación o titularidad para detener el crimen.
- Usar el derecho a la privacidad para proteger los datos de los delincuentes es un sinsentido.

- Implica saber que la delincuencia se sirve de la tecnología, mientras que ingenuamente negamos a la policía la posibilidad de acceder a la información que esa tecnología produce.
- La información ni es secreta, ni hay que producirla. Esta en poder de los prestadores de telecomunicaciones o aplicaciones en línea, para fines comerciales.
- Previamente la Ley 29924, que sanciona las llamadas malintencionadas a centrales de emergencias, establecio que la identificación de estas llamadas no constituye una vulneración del secreto de las telecomunicaciones. Nadie la cuestionó.

- Esta ley esta mas cercana al examen de las huellas del delito que de interceptacion de las comunicaciones.

- La proteccion de datos no debería servir para facilitar las cosas a los delincuentes sino exactamente para lo contrario

- De lo contrario no se podría detener a una delincuente porque para ello hay que identificarlo y localizarlo

MUCHAS GRACIAS

José Alvaro Quiroga León

apdp@minjus.gob.pe