LITORALPRESS

Fecha: 04-10-2024
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo A
Tipo: Noticia general
Título: El amplio y debatido uso de los sistemas de intervención de celulares en el mundo

Pág. : 5
Cm2: 593,2
VPE: $ 7.792.879

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Punto de la ley antiterrorista que se tramita en el Congreso chileno:

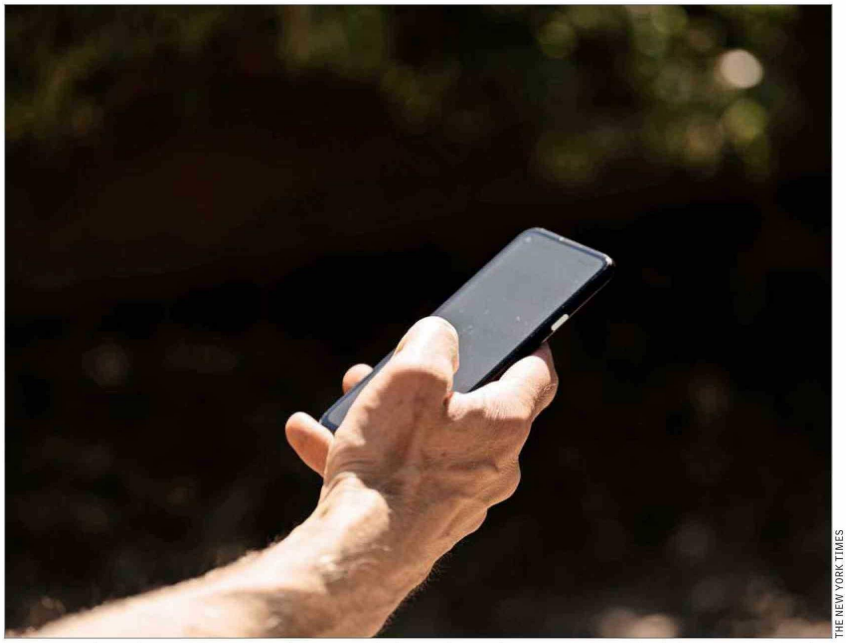
El amplio y debatido uso de los sistemas de intervención de celulares en el mundo

Los dispositivos IMSI catcher, que permiten rastrear teléfonos móviles, han sido implementados por decenas de países para combatir el terrorismo y el crimen, pero preocupan las vulneraciones a la privacidad y su opaca supervisión.

JEAN PALOU EGOAGUIRRE

Las tecnologías de intervención de teléfonos celulares que utilizan los sistemas IMSI catcher, que permiten rastrear la ubicación de dispositivos móviles —y a sus usuarios—, interceptar sus comunicaciones y obtener incluso sus metadatos, han sido usados desde hace muchos años por agencias de seguridad de decenas de países para tareas como el combate al terrorismo o el crimen organizado, aunque siempre con controversia por la preocupación por las posibles vulneraciones a la privacidad y los derechos civiles de las personas. Ese debate se ha instalado ahora en Chile, en medio del trámite en el Congreso de la ley antiterrorista, que contempla en su artículo 19 la interceptación de redes de telefonía móvil por zona geográfica.

Los dispositivos IMSI catcher, también llamados Stingray por un conocido modelo que se fabrica en EE.UU., básicamente son antenas "falsas" que simulan una torre de telefonía móvil, lo que "engaña" a los celulares cercanos que se conectan a ellas. De este modo, su operador accede a los IMSI de los teléfonos —sigla de Identidad Internacional del Suscriptor de Móvil, un número único global—, con lo que puede geolocalizar los aparatos, acceder a sus comunicaciones, enviar mensajes de texto y hasta bloquearlos sin la autorización de la compañía telefónica.



THE NEW YORK TIMES

EN EE.UU. el uso de estos dispositivos ha provocado demandas por la presunta violación de la Cuarta Enmienda.

El caso de EE.UU.

En EE.UU. su uso es extendido en agencias como el FBI, la CIA o el Servicio Secreto, e incluso en departamentos de policías locales y estatales, para rastrear a personas bajo investigación en casos de terrorismo, tráfico de drogas, secuestros y otros delitos graves. Aunque ya se utilizaban desde mucho antes, en 2015 el departamento de Justicia y el departamento de Seguridad Nacional establecieron una política que requiere que las agencias federales obtengan una orden judicial (*warrant*) basada en una causa probable antes de utilizar un IMSI-catcher, aunque hay excepciones en el caso de emergencias que impliquen riesgos inmediatos para la vida o la seguridad pública, un escenario en el cual deben justificar su uso retroactivamente.

"Los dispositivos que imitan estaciones base de teléfonos móviles para engañar a los teléfonos han estado disponibles desde mediados de la década de 1990. Las fuerzas policiales locales de Estados Unidos y el FBI han utilizado estos dispositivos regularmente desde los primeros años de este siglo. Pero la atención mediática y los litigios comenzaron a destacar el uso invasivo de esta tecnología recién a principios de la década de 2010", explicó Eben Moglen, profesor de Derecho de la Universidad de Columbia y experto en ciberseguridad. "Su uso previsto es una invasión de la privacidad, lo que no es un riesgo, es una certeza. Obviamente, si ha de existir el Estado de Derecho, este debe regular el uso de una tecnología intrínsecamente invasiva por parte del poder público", añadió.

En Estados Unidos —donde se usan además dispositivos transportables "de mano" e incluso algunos en aviones— se ha establecido que las agencias de seguridad deben minimizar la recolección de datos no relevantes, esto es, aquellos de personas no investigadas. Pero organizaciones como la American Civil Liberties Union (ACLU) y Electronic Frontier Foundation (EFF) han señalado que es muy opaca la supervisión al respecto, y en tribunales se han presentado varias causas por la violación de la Cuarta Enmienda de la Constitución, que garantiza la privacidad de los ciudadanos.

Protocolos en Europa

La regulación también ha sido un gran tema en Europa, donde existe un mal antecedente por el uso que se le dio esta tecnología en Ucrania en 2014, cuando miles de manifestantes que participaron en las protestas opositoras recibieron luego mensajes de texto en sus celulares con amenazas: habían sido geolocalizados y registrados.

En Francia, los IMSI catchers son usados por varias agencias de seguridad, especialmente en operaciones antiterroristas y de tráfico de drogas. Su funcionamiento se reguló en 2015, tras los atentados terroristas de París, cuando la Ley de Vigilancia estableció los parámetros para su autorización y creó la Comisión Nacional de Control de Técnicas de Información (CNCTR, en francés), que actúa como un organismo de fiscalización.

De manera similar, en Alemania —donde el espionaje interno es un tema sensible, por su experiencia con el régimen nazi y en la ex-RDA— el uso de la tecnología está permitido bajo los términos de la Ley de Vigilancia de Telecomunicaciones, que establece en la mayoría de casos la obligación de una orden judicial previa y la eliminación de los datos de personas que no sean de interés.

En Reino Unido, en tanto, si bien existe una ley que contempla el uso de estos dispositivos, la Investigatory Powers Act 2016, y se asume que la utilizan la Policía Metropolitana y el MI-5, un dictamen de un tribunal sobre libertad de información permitió a las agencias de seguridad "ni confirmar ni rechazar" su aplicación. Sí se sabe que se usaron, por ejemplo, en los alrededores de la embajada de Ecuador en Londres, cuando estuvo refugiado allí Julian Assange.

"El régimen legal de EE.UU. es más sofisticado en torno al uso de IMSI chatchers. Existe cierta jurisprudencia y protecciones constitucionales. En Reino Unido, en cambio, la policía ha jugado al juego de la evasión: no confirman su uso, lo que hace imposible que se regule", dijo a "El Mercurio" Gus Hosein, director de Privacy International, una organización que ha presentado varias demandas en tribunales europeos en contra de su uso.

"Que nuestros gobiernos lleguen al extremo de hacerse pasar por proveedores de redes telefónicas es una gran deshonestidad. Que elijan explotar ese error solo para llevar a cabo vigilancia masiva es una negligencia en su deber de mantener nuestra infraestructura segura y protegida", comentó Hosein. "¿Realmente imaginan los gobiernos que son los únicos que operan un IMSI catcher en sus países? Para ser claros: las interferencias legales con la privacidad son permisibles. Pero el uso de un *exploit* que monitorea a muchas personas no es aceptable en una sociedad democrática", agregó.