Espionaje y acoso en México

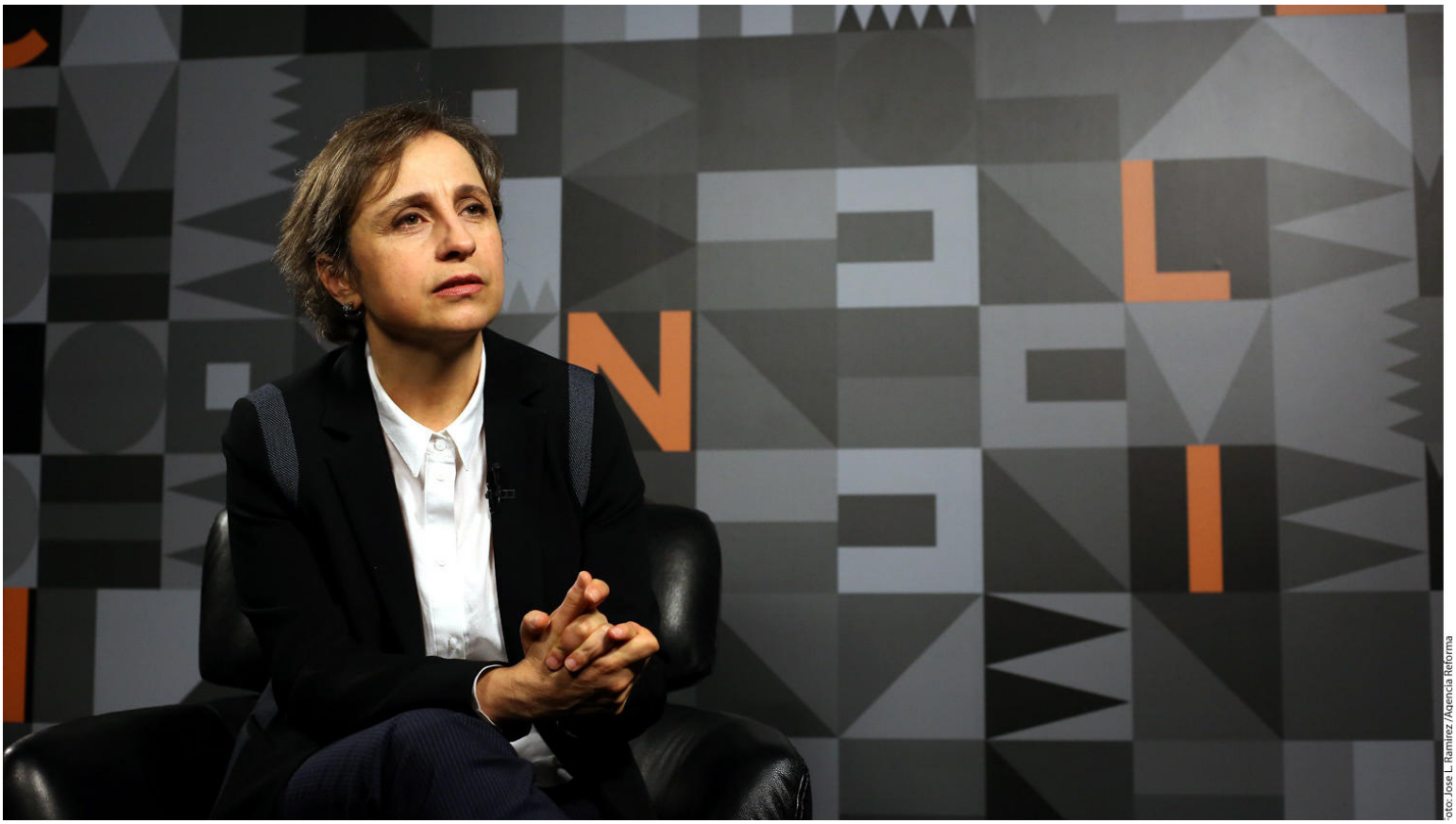

Foto: José L. Ramírez/Agencia Reforma

Enrique Peña Nieto debe comparecer ante el Congreso por el espionaje dirigido contra periodistas y activistas, afirmó la periodista Carmen Aristegui. (José L. Ramírez)

By **Agencia Reforma**
CIUDAD DE MÉXICO

JUNE 26, 2017, 9:51 AM

Las denuncias de espionaje contra activistas y periodistas se acumulan, y abren el debate sobre la necesidad de transparentar la adquisición de tecnología de inteligencia y la urgencia de regular las intervenciones gubernamentales de comunicaciones.

Hasta el momento, se ha confirmado que 16 personas han sido víctimas de espionaje con el malware Pegasus, una herramienta de hackeo antiterrorista comprada por instancias del gobierno mexicano a la empresa israelí NSO Group, un programa que permite intervenir todas las comunicaciones del teléfono celular de un usuario-objetivo.

Según las organizaciones especializadas en derechos digitales, el uso de herramientas de espionaje está completamente acreditado, por lo que piden que se regule y se respeten las leyes en la materia.

El 23 de mayo, una decena de organizaciones de la sociedad civil rompió con el gobierno de Enrique Peña Nieto, al anunciar su retiro de la Alianza para el Gobierno Abierto, una iniciativa de la ONU que vela por la transparencia gubernamental. El rompimiento se dio luego del espionaje contra defensores del derecho a la salud.

En esa ocasión, la Secretaría de la Función Pública respondió con un comunicado en el que pidieron a los activistas presentar las denuncias formales de sus casos de espionaje.

El pasado 19 de junio, activistas y periodistas presentaron nuevas denuncias de espionaje, esta vez ante la PGR, y aseguraron que estas intervenciones se han convertido en una forma de acoso.

La respuesta del gobierno se dio desde la oficina de prensa internacional de Presidencia, que aseguró que no existen pruebas de que agencias gubernamentales sean responsables del supuesto espionaje.

Para los activistas y expertos en derechos digitales, no hay duda de que el gobierno los tiene intervenidos.

'Atacan a quienes luchamos por los derechos'

Lo peor del espionaje del gobierno no es que use herramientas invasivas de alta tecnología, sino que las usa contra defensores de derechos de las personas y no para el combate al crimen organizado, asegura Alejandro Calvillo, director de El Poder del Consumidor.

"El gobierno ha estado espiando a quienes estamos luchando por la justicia, por el derecho a la salud y por los derechos humanos", denuncia.

Calvillo resalta que el gobierno tiene el derecho de emplear tecnología en labores de inteligencia, pero no de usarla ilegalmente.

El defensor de derechos del consumidor en productos alimenticios fue, junto con Simón Barquera y Luis Encarnación, uno de los primeros tres activistas que denunciaron ser víctimas de espionaje en México.

Su caso permitió que tres organizaciones, la Red por los Derechos Digitales (R3D), Social Tic y Citizen Lab, comprobaran el uso del malware Pegasus, fabricado por la empresa israelí NSO Group, que es vendido exclusivamente a gobiernos.

Aunque la PGR ha admitido la adquisición de este programa, ha rechazado que lo esté utilizando; sin embargo, para Calvillo no hay duda del uso que se le está dando a esta herramienta.

"Este tipo de acciones, no puedes pensar más que vienen de adentro del gobierno mexicano, de funcionarios del gobierno mexicano, que te están tratando de espiar; no solamente tener acceso a tus llamadas, es tener acceso a tus archivos, tus fotos, a tu teléfono, tu cámara", asegura.

En su experiencia, este tipo de espionaje ha implicado más que saberse víctima de una escucha telefónica, los dos mensajes que le enviaron tratando de instalar malware se convirtieron en una intimidación.

"Sientes inseguridad por lo que te puede pasar. Saben dónde estás, saben la información que tienes, saben tus contactos, saben si tienes otros familiares; tienen acceso a todo. Te sientes totalmente vulnerable", resalta

Los mensajes enviados a Alejandro Calvillo remitían a un sitio en el que se alojaba el malware Pegasus. El envío de los mismos se dio en un momento en que Calvillo trabajaba en contra de una regulación en materia de salud (julio de 2016), lo que para el investigador es una muestra de que la corrupción dentro del gobierno ha permitido a las empresas actuar contra activistas vía espionaje.

"Tienes funcionarios dispuestos a actuar a favor de intereses económicos. Esto se ha utilizado contra muchas organizaciones que trabajan en otras áreas de derechos o en cualquier área que moleste al Estado", detalla.

Además del peritaje de la Universidad de Toronto que confirma que se utilizó esta herramienta, el silencio del gobierno ante la denuncia es, para el investigador, una señal de que el gobierno fue descubierto.

Considera que su caso sirvió para que otras personas espiadas supieran lo que estaba pasando y también denunciaran. Espera que, además de los 12 casos documentados por R3D, Citizen Lab y Social Tic (difundidos la semana pasada en The New York Times), más organizaciones y periodistas denuncien.

"Lo único que nos toca a nosotros es salir a la luz y denunciarlo. Y fue una buena noticia que el grupo de gobierno abierto saliera a denunciar. Es sentirte que no estás solo y que la sociedad civil diga: tenemos que estar unidos en contra este tipo de prácticas", pide.

'Peña Nieto debe comparecer'

Enrique Peña Nieto debe comparecer ante el Congreso por el espionaje dirigido contra periodistas y activistas, afirma la periodista Carmen Aristegui.

"El presidente de la República, como jefe de Estado, es el responsable de todas las instancias de gobierno que tienen en sus manos la utilización de estos mecanismos de espionaje. El Presidente no puede estar ajeno a la conducta de sus agentes del Estado, y mucho menos puede estar ajeno al producto de sus espionajes", declara.

Aristegui se ha caracterizado por su crítica hacia el peñismo; coordinó y publicó la investigación La Casa Blanca de Peña Nieto, un reportaje que reveló conflictos de interés entre el Presidente y el Grupo Higa, y tuvo que dejar su programa radiofónico, acusando presiones del gobierno hacia MVS para sacarla del aire. Ella, sus colaboradores y hasta su hijo -menor de edad- también fueron víctimas de espionaje.

La periodista considera que si el Presidente no sabía del espionaje y es inocente, debe decirlo.

"¿Por qué no sale a decir que está indignado?, ¿por qué no sale a decir lo que esperaríamos de un Presidente inocente? Me parece que todo lo incrimina, que todo conduce a él. Que los temas relacionados con las personas que han sido atacadas están relacionados, todos, con asuntos de primer orden del gobierno federal; por eso, cuando de comparecencia se habla, claro que tiene que ir el director del Cisen, el procurador General de la República, tiene que ir Osorio Chong; claro que tendría que ir el Presidente de la República", expone.

El reporte de Citizen Lab precisa que Aristegui, su hijo y dos de sus colaboradores -Rafael Cabrera y Sebastián Barragán-, recibieron al menos 56 mensajes de un total de 76 intentos de infección comprobados.

Los ataques se dividen en dos momentos: de enero a octubre de 2015, con 18 mensajes vía SMS, y de febrero a agosto de 2016, cuando les llegaron 38 más.

"Este grupo de periodistas está y ha estado en el foco de la atención del presidente Peña Nieto y su gobierno. Esta voluminosa cantidad de ataques -decenas de ataques a nuestras personas, a nuestros equipos móviles- nos habla de una situación de temor a nuestro trabajo, de inquietud del poder de ser descubiertos en algo", afirma.

El primer intento de infección fue enviado a Aristegui el 12 de enero, dos meses después de que fue publicado el reportaje de la casa del Presidente. El último mensaje de la primera etapa le llegó el 25 de octubre, tres semanas después de que el reportaje fue publicado como libro. La cercanía entre los intentos de infección con las fechas de los trabajos publicados evidencia el origen de los mismos; por eso, Aristegui demanda la investigación.

"Hay que acudir a las instancias legales, exigir que se cumplan las leyes. Después, acudir a instancias

internacionales", señala.

La periodista espera que el Congreso se ponga de lado de quienes padecieron los intentos de espionaje.

"Vamos a ver también de qué tamaño es el Congreso. Vamos a ver qué tipo de reacción hay de la clase política que empieza a darse cuenta de que también han sido espiados. Es de esperarse que esto se convierta en el más grande escándalo de Peña Nieto al final de su sexenio", advierte.

'Se nos trata como enemigos del Estado'

Un gobierno que espía a quienes están luchando contra la corrupción tiene que ser un gobierno corrupto, argumenta Juan Pardinas, director del Instituto Mexicano para la Competitividad.

Usar tecnología del gobierno para intervenir las comunicaciones de promotores de políticas anticorrupción, defensores de derechos y periodistas es convertir a estos promotores en enemigos del gobierno.

"Somos tratados como enemigos del Estado, pero no somos los enemigos del Estado. Los enemigos del Estado son los huachicoleros, el crimen organizado y, por el absurdo de la prohibición de las drogas, los narcotraficantes".

Confirmado el uso de la herramienta de espionaje en contra de 16 personas, Pardinas pide que el Congreso promueva y no bloquee las indagatorias. Y fija la responsabilidad en dos personajes clave.

"Uno es Pablo Escudero, del Partido Verde, presidente del Senado, y otro es César Camacho, líder del PRI en la Cámara de Diputados. Ellos dos, del PRI y el Verde, los partidos que conforman la coalición que gobierna desde Los Pinos, deben dejar de comportarse como guardaespaldas del espionaje realizado desde el gobierno.

"Esperaría que se llamara a una comparecencia al secretario de Gobernación, como encargado de los órganos de inteligencia del país; al procurador general de la República, que tiene el acceso a este software y tiene la responsabilidad de investigar la denuncia ya presentada".

Compara el escándalo mexicano de Pegasus, con lo que sucede en Estados Unidos: al conocerse la probable intervención del gobierno ruso en las elecciones de ese país, se llamó a comparecer ante el Congreso a funcionarios del gabinete de Donald Trump.

"Aquí no tenemos este fogueo de cuestionar a los funcionarios, y el PRI y el Verde lo que hacen es evitar que se les toque con el pétalo de una pregunta incómoda".

Para el director del IMCO, la división y equilibrio de poderes que debe prevalecer para esta investigación pone sobre la mesa el debate que asegure que el próximo fiscal general de la República cuente con autonomía.

"Es como el conflicto de interés de Virgilio Andrade como secretario de la Función Pública, que tenía que investigar a su jefe. Aquí, la PGR va a tener, punto A, que investigarse a sí misma o, punto B, investigar a un compañero de gabinete del procurador".

Preocupado por estar entre quienes fueron espiados con el programa Pegasus, Pardinas reconoce que estas herramientas deben ser utilizadas por el Estado, pero en contra de la delincuencia.

"En un Estado que está enfrentando amenazas como el huachicol en Puebla, el crimen organizado en Tamaulipas, los feminicidios en el Estado de México, secuestros en distintas partes del país, estos instrumentos son válidos para una investigación policial", resalta.

Además de Pardinas, su colaboradora en el IMCO, Alexandra Zapata, también recibió mensajes para infiltrar su teléfono con el malware Pegasus. Ambos han sido promotores de la Ley 3 de 3, que busca que todos los funcionarios públicos hagan pública sus declaraciones patrimonial, fiscal y de intereses.

La organización que Pardinas dirige también ha sido promotora del nuevo Sistema Nacional Anticorrupción, han demandado que éste garantice independencia de partidos y de los poderes del Estado. Y justo dos de los partidos que han bloqueado el avance de las políticas que promueve IMCO han sido el PRI y el Verde.

Tras la irrupción de este escándalo, el investigador opina que deberían transparentarse los contratos de compra de estos programas espía, una explicación sobre cómo se ha utilizado el espionaje, y que no se frenen las iniciativas anticorrupción.

"En México, la transgresión y rompimiento del Estado de Derecho comienza por las autoridades. La autoridad pide que los ciudadanos nos comportemos de acuerdo con lo establecido en la ley, pero esa autoridad no es capaz de cumplirla", afirma.

'Vigilancia fuera de control'

Antes se tenía la sospecha de que el gobierno mexicano realizaba espionaje, ahora se tiene la confirmación de que posee las herramientas y las está utilizando, asegura Luis Fernando García, director de la Red por los Derechos Digitales (R3D), quien pide que se regule y se respete la Ley Federal de Telecomunicaciones y la Ley de Protección de Datos Personales.

"La información que hemos estado recabando a lo largo de tres años demuestra un incremento en la utilización de facultades de vigilancia y la intervención de comunicaciones por parte del Estado mexicano", detalla.

Entre los años 2013 y 2015, R3D presentó 3 mil 182 solicitudes ante autoridades judiciales para conocer la cantidad de intervenciones de comunicaciones; sólo 573 tuvieron respuesta. Para 2016, la organización incrementó a 3 mil el número de solicitudes.

García indica que el espionaje con este tipo de herramientas se ha incrementado, pues no se necesita la colaboración de empresas de telecomunicaciones. Se compra el software y se lanza la estrategia. La cantidad de ataques depende de la cantidad de dinero que se tenga.

Explica que en estos ataques hay una triple ilegalidad: primero, se realiza sin autorización judicial; segundo, lo practican dependencias que no tienen facultades y, tercero, no se utiliza para combatir el crimen organizado, sino en contra de personas que tienen una postura política opuesta al gobierno.

"Se supo que muchas autoridades en el país, incluso que no tienen facultades, como Pemex, gobiernos estatales, como los de Puebla, Jalisco, Tamaulipas y Querétaro no tienen facultades para vigilar. Los únicos que pueden llevar a cabo una intervención de comunicaciones privadas para prevenir delitos son la Policía Federal, la Procuraduría General de la República y las procuradurías locales y el Cisen, cualquier otra autoridad que haya adquirido estas herramientas, de entrada, es ilegal su adquisición, y hay mucha evidencia de que otros han comprado y no ha habido una investigación oficial", asegura.

Adicionalmente, el director de R3D confirma que ha habido un incremento importante en el gasto del gobierno mexicano en este tipo de programas. Detalla que primero se compró software a la empresa italiana Hacking Team, y que fue tanta la explotación del mismo que México se convirtió en el principal cliente de esa firma.

De 35 países que se pudo detectar que en 2015 habían comprado herramientas a Hacking Team, México lideró como el primer cliente con un gasto de 5.8 millones de euros; le siguieron Italia con 4 millones; Marruecos con 3.1; Arabia Saudita con 2.4 y Chile con 2.2

Explica que se desconoce si las intervenciones con los programas vendidos por NSO Group o Hacking Team están vinculadas con los casos de espionaje que se han aceptado públicamente por instancias de gobierno, vía solicitudes de transparencia.

La imposibilidad de vincular estos casos con los expedientes es porque las solicitudes de información se

entregan incompletas y los casos de espionaje no se reportan con la referencia de algún expediente judicial. Adicionalmente, las cifras difieren entre las autoridades.

"Hay discrepancias en los números. Cuando le pides a una fiscalía, a una procuraduría, cuántas veces ha solicitado la intervención de comunicaciones privadas, te dan una cifra; cuando vas con los jueces y le preguntas cuántas veces ha venido la fiscalía y la procuraduría a pedirte la autorización, te dice que ninguna, y la fiscalía, por ejemplo de Jalisco, te dice que dos o tres veces en dos años. Y, justamente, la Fiscalía de Jalisco, el gobierno de Jalisco, alega que contrató el malware de Hacking Team. Hay dos opciones: o la Fiscalía de Jalisco gastó millones de pesos en adquirir un malware de vigilancia que ha utilizado tres veces en el mejor de los casos, o compró este malware y no lo está usando o lo está usando de manera ilegal", resalta.

El activista afirma que el gobierno no tiene una respuesta con la que compruebe contundentemente que no tiene responsabilidad en el espionaje.

"Los hemos cachado con las manos en la masa y no tienen forma de defenderse y no existen contrapesos institucionales, no existe una Fiscalía, una Procuraduría con voluntad política para investigar, el INAI tampoco. Es clara la evidencia, es incontrovertible que los mensajes trataban de infectar los celulares con el malware Pegasus de NSO. Es incontrovertible documentalmente que, al menos la Sedena y la PGR, poseen este malware; están los documentos, los contratos. No sabemos si hay más autoridades, pero el hecho de que estén guardando silencio genera mucha más suspicacia respecto de qué otras cosas hay detrás", considera.

Agrega que otro tema que debe ponerse sobre la mesa es la parte ética en el uso de la tecnología: debatir por qué el gobierno mexicano se aprovecha de las vulnerabilidades de un sistema, en lugar de avisarle a los fabricantes para evitar el espionaje.

'El fin es espiar, no proteger'

El gobierno mexicano está comprando tecnología con el único objetivo de espiar a sus oponentes, asegura Sergio Araiza, miembro del equipo de Social Tic, organización que colaboró con R3D y Citizen Lab en la detección del malware Pegasus contra activistas.

"El gobierno mexicano lleva varios años comprando tecnología de espionaje de manera sistematizada; además, participa en círculos en los que se busca dotar de tecnología nueva, sofisticada e intrusiva para obtener, de manera ilegal, datos de las personas", asegura.

Comenta que la evidencia muestra que el programa Pegasus sí puede ayudar en labores de vigilancia, pero

lamentablemente esta herramienta no se está aplicando a cuestiones de seguridad, por lo que urge a transparentar y reglamentar su uso.

"El problema no radica en el acceso a esta tecnología, pues todos los gobiernos requieren de acciones de inteligencia para combatir todo tipo de amenazas que atenten contra la seguridad nacional o la seguridad del interior, el problema radica en que no existen mecanismos de control, de auditoría y, evidentemente, de impartición de justicia donde se hagan revisiones sobre quién tiene acceso a esta tecnología, cuándo se está usando y contra quién se está usando.

"Y por lo menos una clase de evaluación del resultado del uso de esta tecnología. Si pensamos desde esa perspectiva, lo cierto es que el gobierno se ha pasado cualquier cantidad de candados constitucionales con el ánimo de utilizar este tipo de herramientas", detalla.

Comenta que se sabe del uso del programa vendido por NSO Group, pero seguramente hay otros en manos del gobierno.

"No sólo se remite a este proveedor, sino a otros. Teníamos el caso de Think Spy; el año anterior teníamos el caso de Hacking Team, y éste tenemos el caso de NSO Group. Hay evidente inversión de los gobiernos en alta tecnología de espionaje y de que ésta se utiliza fuera del marco de la ley", asegura.

Explica que la denuncia de las organizaciones no sólo se queda en exponer los casos de espionaje sino en la demanda de una actuación por parte de las autoridades

"Está en sus ámbitos, tanto del INAI como de la PGR, tienen capacidad para activar investigaciones independientes sin necesidad de presentar denuncias. El llamado es a transparentar esta situación. Se sabe que el gobierno ha adquirido tecnología, hay documentos en donde existen conversaciones y negociaciones del gobierno para comprar esta nueva tecnología, la misma empresa israelí ha mencionado que sólo se vende al gobierno. Esperamos que esto no sólo se remita a los casos denunciador por las organizaciones de la Alianza para el Gobierno Abierto. Estamos seguros que se ha afectado a otra capa de personas, de todos los niveles en toda la República", detalla.

'Intervienen sin autorización'

El espionaje no sólo se hace con alta tecnología, sino también se propicia porque empleados de compañías telefónicas entregan metadatos y clonan los teléfonos celular sin ninguna autorización judicial, asegura Cédric Laurant, director de SonTusDatos.org.

"Idealmente, la información de los metadatos de los celulares tendría que utilizarse con el propósito de evitar crímenes como el secuestro o el terrorismo, pero, por el tema de la corrupción, se utilizan sin ninguna justificación o autorización de un juez", detalla.

Los metadatos de cada celular que está en funcionamiento en México los guardan las empresas de telefonía por dos años. Esta información permite conocer todas las actividades de un usuario sin instalar un programa de espionaje.

Paradójicamente, los datos no están disponibles para los propios usuarios.

La organización SonTusDatos ha hecho el ejercicio de solicitar los metadatos, pero las compañías telefónicas se niegan a proporcionarlos.

"El derecho a los datos personales no es proporcional a la facultad que se le da a las autoridades. Se dio la facultad a las empresas de telecomunicaciones de que guardaran estos datos y se dio la facultad al gobierno para pedirlos para casos de terrorismo, narcotráfico, pero las facultades no son respetadas", asegura.

Resalta que ha sido tal la irregularidad en el uso de solicitar metadatos que existe un mercado negro en internet.

Detalla que personal gubernamental, sin tener las atribuciones, los solicita y después de obtenerlos los utiliza para labores de espionaje o los vende a quien se los solicita.

Adicionalmente, destaca que existe otro mercado, el de clonación de líneas de teléfonos celulares, algo que también se da por la corrupción.

Se hace la clonación para escuchar, para recibir los mensajes SMS o para obtener los registros de todas las llamadas de una línea, lo que se conoce como sábana telefónica.

Laurant denuncia que un informante del que tiene el compromiso de resguardar su identidad le mostró otro programa de espionaje comprado por el gobierno. El sistema se llama "Lighthouse" y permite la geolocalización, obtener datos personales del objetivo. El programa no es detectable en el aparato.

Basta tener el número IMSI (International Mobile Subscriber Identity), que es el código asignado por un operador de telefonía a la línea de una persona, este número funciona como si fuera la dirección del teléfono, por lo que a partir del mismo se puede hacer la geolocalización del usuario.

La falla, detalla Laurant, es que en México se permite el almacenamiento de los metadatos, algo que en

Europa quedó prohibido para evitar la vulnerabilidad de la información.

"En Europa, hubo un error de permitirlo; en 2006, se estableció los criterios bajos los cuales se podía acceder a esos metadatos. Dependiendo del Estado miembro, se podían tener de seis a 24 meses, pero esta directiva fue invalidada en junio de 2014 por la Corte de Justicia de la Unión Europea, en Luxemburgo. Un mes después de este fallo de la Corte Europea de Justicia, el legislador, aquí, con la Ley Federal de Telecomunicaciones, toma disposiciones que permiten almacenar los datos por dos años", detalla.

This article is related to: Tornadoes and Wind Storms