



INTER PRESS SERVICE
Agencia de Noticias

Periodismo y comunicación para el cambio global

América del Norte, América Latina y el Caribe, Ciencia y tecnología, Ciudadanía en movimiento, Crimen y justicia, Democratización, Derechos humanos, Destacados, Europa, Geopolítica, Globalización, Gobernanza mundial, Las elegidas de la redacción, Libertad de prensa, Mundo, Sociedad Civil, Últimas Noticias

México víctima y victimario de espionaje

Por Emilio Godoy



Imagen de recopilación mundial de datos de SNA. El verde indica la menor vigilancia, seguido de amarillo, naranja y rojo, el más alto. Crédito: Creative Commons

**MÉXICO, 30
may 2014 (IPS)**
- Descontrol,
falta de
regulación y
opacidad
distinguen el
monitoreo y la
intervención de
las

comunicaciones electrónicas en México, un año después de las revelaciones sobre esas prácticas que sacudieron al mundo.

Este país latinoamericano, de casi 118 millones de habitantes, ha sido uno de los objetivos de la ciberintrusión masiva e ilícita de la estadounidense Agencia Nacional de Seguridad (NSA, por sus siglas en inglés). Pero a esa intrusión clandestina no se respondió con cambios sustanciales para evitar interceptaciones.

"No hay legislación sobre vigilancia e intervención, ni buenas prácticas de las empresas. Hay un vacío legal. Pueden estar recabando metadatos", denunció a IPS el activista Jesús Robles, de la no gubernamental Propuesta Cívica.

Los metadatos son la información asociada, por ejemplo, a un mensaje de correo electrónico o a una llamada telefónica, como quién emite y quién recibe, dónde, a qué hora y con qué duración.

El 5 de junio de 2013, el diario británico The Guardian reveló que la NSA recogía información de usuarios dentro y fuera de Estados Unidos, en este caso requerida al operador de telefonía móvil Verizon Business Network Services, el mayor de ese país.

Fue el comienzo de una serie de revelaciones sobre las operaciones secretas de esa agencia, que realizó Edward Snowden, excontratista de la Agencia Central de Inteligencia de Estados Unidos (CIA), actualmente asilado en Rusia.

La NSA usó el programa informático Prism para espiar a varios países, entre ellos México, sobre asuntos como combate antidrogas, energía, seguridad y política interna.

Además, con el programa Blarney, Estados Unidos intervino las comunicaciones de varias embajadas en Washington, entre ellas la mexicana. Mediante otra herramienta, Boundless Informant, captó ilegalmente llamadas y correos electrónicos que pasaron por las redes de telecomunicaciones estadounidenses.

El periodista estadounidense Glenn Greenwald reveló el 1 de septiembre de 2013 que la NSA había espiado en 2012 las comunicaciones electrónicas de la presidenta de Brasil, Dilma Rousseff, y de su homólogo de México, Enrique Peña Nieto, en este caso durante la campaña electoral que lo llevó a la Presidencia.

Estados Unidos ha ignorado las protestas mexicanas, que incluyeron una nota diplomática con el reclamo de una investigación y una condena del bicameral Congreso legislativo.

El medio digital estadounidense The Intercept, dirigido por Greenwald, dio a conocer el 19 de este mes que el programa ilícito Mystic recolecta metadatos de los casi 100 millones de teléfonos celulares operativos en México.

"No se ha hecho mucho. Si la sociedad supiera más, podría presionar más a las empresas nacionales y extranjeras para que a su vez presionen más al gobierno", declaró a IPS el especialista Cédric Laurant, uno de los cuatro fundadores de la no gubernamental Son Tus Datos, dedicada desde 2012 a difundir la necesidad de proteger la privacidad en las comunicaciones.

México también adquirió programas informáticos para grabar voces, rastrear llamadas telefónicas, correos electrónicos, charlas digitales, visitas a páginas de Internet y redes sociales.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares garantiza desde 2010 el derecho a la privacidad y establece que, si una institución desea transferir esa información a terceros nacionales o extranjeros, deberá comunicarlo a los usuarios dueños de la información junto con el propósito para el que se autoriza,

Pero esa garantía quedó minimizada con la entrada en vigor en marzo de 2012 de la Ley de Geolocalización, que permite al gobierno recolectar, sin aviso alguno y en tiempo real, datos geográficos de usuarios de teléfonos móviles.

Además, el Código Nacional de Procedimientos Penales, vigente desde marzo, permite a las autoridades acceder a datos de geolocalización en vivo y sin autorización previa de un juez

El laboratorio interdisciplinario Citizen Lab de la Universidad de Toronto, en Canadá, informó en marzo de 2013 sobre el hallazgo de dos servidores del programa intrusivo FinFisher, fabricado por la empresa británica Gamma Group, en redes de dos compañías mexicanas de telefonía: Iusacel y Uninet, filial de Teléfonos Mexicanos (Telmex).

Tras este hallazgo, Propuesta Cívica y ContingenteMX, una organización que defiende los derechos humanos digitales, solicitaron al estatal Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) una investigación a la empresa Obses de México sobre el uso de ese programa.

El IFAI aprobó en marzo sanciones para la empresa mexicana Obses por vender FinFisher a entidades gubernamentales.

Los tribunales de Gran Bretaña condenaron el 12 de mayo la decisión de la Oficina de Aduanas e Ingresos de no investigar la posible ilegalidad de la exportación de FinFisher por la subsidiaria internacional de Gamma Group, lo cual abre el camino para una revisión de las ventas al exterior del programa.

En febrero, Citizen Lab volvió a la carga con dos informes sobre utilización de programas espías. En uno de ellos – "Mapeando los programas espía ir rastreables de Hacking

Team", se indica que agencias de 21 países usan o usaron el Sistema de Control Remoto (RCS, por sus siglas en inglés), entre ellos México, Colombia y Panamá.

RCS puede copiar archivos de una computadora, grabar llamadas por la aplicación digital Skype, correos, mensajes de texto y contraseñas y puede encender cámaras y micrófonos para espiar a su objetivo. Está destinado únicamente a gobiernos.

El informe habla de la existencia de al menos cuatro servidores en México vinculados con empresas privadas que componen un circuito electrónico para ocultar la ruta del espionaje.

El documento "El nexo de Hacking Team con Estados Unidos", también de Citizen Lab, identificó al menos 12 casos de centros de datos con sede en ese país que pertenecen a una estructura de espionaje fuera de esa nación. Esos servidores parecen cooperar con 10 países, entre ellos México y Colombia, en espionaje y operaciones legales o clandestinas.

Citizen Lab halló 14 direcciones IP (protocolo de Internet que distingue cada dirección en la red), de las cuales 12 seguirían activas.

En el reporte anual 2013 de la Iniciativa de la Red Global (GNI, por sus siglas en inglés) se citan los casos de Argentina, Brasil y México, pero sin suministrar detalles.

GNI, integrada por gobiernos, académicos y empresas de Internet, evaluó a Google, Microsoft y Yahoo! a partir de 59 expedientes, de los que 47 involucraban una petición gubernamental, 30 eran sobre privacidad y 17 sobre libertad de expresión.

El documento informa de 29 casos de petición de datos del usuario, 11 de criminalización de una expresión legítima y 10 de bloqueo o filtro de la conexión.

La legislación mexicana no obliga a las empresas de telecomunicaciones a revelar solicitudes del gobierno sobre actividades de los usuarios de la red.

"La intervención no ha probado su eficacia, hay vulneración de derechos", resaltó Robles.

"Hay que concientizar al usuario para que, con un número mayor, esa masa pueda hacer presión sobre las empresas, y que el usuario tome la privacidad en sus manos con las nuevas herramientas", planteó Laurant.