INTER PRESS SERVICE
Agencia de Noticias

Periodismo y comunicación para el cambio global

América Latina y el Caribe, Ciencia y tecnología, Crimen y justicia, Derechos humanos, Destacados, Libertad de expresión, Sociedad Civil, Últimas Noticias

Espionaje opaca la nueva estrategia mexicana de ciberseguridad

Por Emilio Godoy

Estudiantes de una universidad en el estado de México, contiguo a la capital del país, revisan sus teléfonos móviles. Los ciudadanos del país van a contar con una estrategia para garantizar la ciberseguridad en las actividades digitales. Crédito: Emilio Godoy/IPS

MÉXICO, 8 ago 2017 (IPS) - El gobierno mexicano impulsa la Estrategia Nacional de Ciberseguridad con un enfoque de derechos humanos, mientras que enfrenta acusaciones de espionaje en contra de activistas por el derecho a la salud y contra la corrupción, periodistas, abogados y defensores de derechos humanos.

Esa contradicción ha devenido en un entorno de desconfianza entre la cibercomunidad del país sobre los alcances reales de la nueva política.

El texto final de la Estrategia se conocerá este mes, después que acaben las consultas públicas sobre su borrador, realizadas por un mes y que concluyen el viernes 11.

Entre los seis principios de ese borrador al que tuvo acceso IPS destacan el de los derechos humanos, la gestión de riesgos el fomento de la innovación y la participación "abierta, multisectorial y colaborativa de los diferentes actores y sectores interesados".

El documento, de 13 páginas, impulsa el "uso de las TIC (tecnologías de la información y la comunicación), incluyendo el ciberespacio, de manera libre, confiable, segura y resiliente", pero sin aludir en su texto a las prácticas de espionaje denunciadas por activistas.

Eso sí, en varias partes alude al fomento del "ejercicio libre, seguro y confiable de las TIC".

Cédric Laurant, director ejecutivo de la no gubernamental Artículo 12, cuestionó a IPS la doble moral del gobierno del conservador Enrique Peña Nieto, al señalar que si realmente quiere respetar los derechos humanos debe frenar el espionaje arbitrario.

"Es necesario que se agregue la confianza a la estrategia, pues su fomento apoyará el crecimiento de actividades digitales. Mientras más confianza exista, habrá más uso seguro de la tecnología", dijo el experto, cuya organización toma el nombre del artículo de la Declaración de Derechos Humanos que protege la vida privada y la reputación de las personas.

La desconfianza la abonan revelaciones sobre que la Procuraduría (fiscalía) General de la República, el estatal Centro de Investigación y Seguridad Nacional y la Secretaría (ministerio) de la Defensa Nacional adquirieron el programa de intrusión Pegasus, fabricado por la empresa israelita NSO Group.

> "(en materia de ciberseguridad) hay una corresponsabilidad entre todos los sectores, pero no hay un trabajo integral. Se necesita corresponsabilidad y una estrategia multisectorial en la que todos participen": Anahiby Becerril.

Ese programa infecta los teléfonos móviles de los blancos elegidos mediante un enlace malicioso que, una vez ejecutado, interviene todo el dispositivo, incluyendo mensajes de texto, chats, correos electrónicos y navegación por Internet.

En seis informes publicados desde febrero, Citizen Lab, centro de investigación cibernética adscrito a la Escuela Munk sobre Asuntos Globales de la canadiense y pública Universidad de Toronto, demostró que un grupo de al menos 21 personas recibió en 2015 y 2016 en México docenas de mensajes de texto infectados con Pegasus.

El grupo lo integraban defensores de derechos humanos, activistas anticorrupción y por los derechos de la salud, abogados, dirigentes políticos, científicos, funcionarios públicos e internacionales.

México es el mayor comprador latinoamericano de equipos espías, de acuerdo a como lo que se reveló en los correos electrónicos que en 2015 se hackearon a la fabricante italiana Hacking Team y que distribuyó el sitio Wikileaks.

A criterio de Anahiby Becerril, experta de la no gubernamental Academia Multidisciplinaria de Derecho y Tecnologías, la ciberestrategia del gobierno mexicano debe garantizar la observancia de los derechos humanos.

"Hay una corresponsabilidad entre todos los sectores, pero no hay un trabajo integral. Se necesita corresponsabilidad y una estrategia multisectorial en la que todos participen", declaró Becerril a IPS.

El borrador de la nueva estrategia, elaborado con ayuda del Programa de Seguridad Cibernética de la Organización de Estados Americanos (OEA), estipula la armonización de las leyes para regular las ciberactividades y dotar de "seguridad y confianza" al usuario al efectuar transferencias de datos, comercio electrónico y cualquier actividad digital.

La estrategia "deberá proteger los derechos fundamentales, la salud y las actividades económicas y sociales de los ciudadanos", asegura el texto provisional.

La ciberestrategia incluye la recopilación y actualización de estadísticas sobre uso y confianza de servicios de comercio electrónico y generar indicadores sobre incidentes cibernéticos.

Además, también plantea la armonización de la tipificación de ciberdelitos en el marco legal mexicano y la construcción de un Catálogo Nacional de Infraestructuras Críticas de la Información.

Las instalaciones estratégicas prestan servicios de energía, agua, salud, financieros y comunicaciones, que en total México totalizan unas 2.300.

Pero el borrador presenta también problemas. Su adopción solo será obligatoria para el Ejecutivo federal, pero opcional para los otros órdenes de gobierno, el sector privado y la sociedad, algo muy similar al enfoque adoptado en Estados Unidos.

Además, los talleres del 12 y 13 de julio sobre el contenido de la estrategia, organizados por el gobierno mexicano y la OEA, apenas contaron con presencia de representantes académicos y de la sociedad civil, a pesar de presentarse como parte de su postura “abierta, multisectorial y colaborativa”.

Organizaciones de la sociedad civil planean enviar comentarios sobre la estrategia respecto al espionaje ilegal, la protección de derechos digitales y el riesgo de que tipificar conductas cibernéticas coarte el derecho a una Internet libre y abierta.

Atrapados en la red

El documento reconoce “la complejidad” en la gestión de la ciberseguridad, para la cual esboza 32 acciones en materia de economía, gobierno, seguridad nacional y sociedad.

Entre ellas aparecen concienciación, cultura y prevención; desarrollo de capacidades; cooperación y colaboración; investigación y desarrollo; estándares y criterios técnicos; protección de infraestructuras críticas de información; marco jurídico y medición y evaluación de las políticas.

De hecho, México figura entre los países más atacados por los ciberdelitos. En su reporte sobre incidentes del primer trimestre del año, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros reseña que los robos de identidad y fraudes cibernéticos totalizaron 1,5 millones de casos.

Eso representa 10 por ciento más que en el mismo lapso de 2016, cuando se reportaron unos 1,4 millones de incidentes. El “phishing”, el vocablo inglés que define el robo de identidad, creció más del promedio, 18 por ciento, al saltar de 16.085 a 19.004 casos.

En los tres primeros meses de este año, el promedio mensual de fraudes en el comercio electrónico ascendió a 193.000 casos, cuando hace un año se situó en 131.000. La banca móvil registró un récord de fraudes cibernéticos, con 3.682 sucesos.

América Latina está rezagada en ciberseguridad, como lo exhibe el Índice Global de Ciberseguridad, divulgado en julio por la Unión Internacional de las Telecomunicaciones, un órgano de las Naciones Unidas, que asignó a la región un promedio de 0,26, en una escala en la que 0 es el resultado mínimo y 1 el máximo.

México, donde hay 65,5 millones de cibernautas en una población total de 129 millones de personas, se sitúa al frente de la región, en el puesto 28 con un indicador de 0,66, en un listado mundial encabezado por Singapur.

Bahamas, Chile, Colombia, Dominica, Jamaica, Panamá, Paraguay y Trinidad y Tobago son los países latinoamericanos y caribeños que contaban hasta ahora con políticas oficiales de ciberseguridad dentro de la región, hasta ahora que se sumará México.

En los talleres preparatorios y de debate sobre la nueva estrategia, la industria tecnológica defendió el modelo de autorregulación que ha predominado hasta ahora, sin que haya funcionado, como lo prueba el caso de Estados Unidos.

Además, la industria tecnológica, bancaria y de comercio digital quiere impedir que se le achaque responsabilidad legal en casos de violación de la privacidad de los datos.

A Laurant le preocupa la exclusión de la sociedad civil y la academia, el carácter voluntario de la estrategia y el énfasis excesivo sobre la responsabilidad del cibernauta.

“La industria tiende a decir que el usuario tiene que ser educado, pero no aplica esas prácticas. No se trata solo de educar al usuario, sino también a la industria. Además, debe ser obligatorio que las empresas revelen violación de la privacidad de los datos (data breaches, en inglés)”, cuestionó.

En marzo, la Policía Federal lanzó la campaña “México Ciberseguridad 2017”, con el propósito de fortalecer una cibercultura responsable.

Editado por Estrella Gutiérrez