Surge mercado de ‘software’ para espionaje

Por: La Jornada. 02/08/2016

Lima. Por un módico precio, gobiernos que acostumbran a sofocar la disidencia con arrestos y golpizas, o que abusan de su poder de otros modos, compran *software* de espionaje listo para usar que les permite vigilar conversaciones telefónicas y seguir los movimientos de miles de sus ciudadanos, según una investigación de Associated Press.

Este *software* conocido como de *interceptación legal*, disponible desde hace años para policías occidentales y agencias de espionaje, resulta ahora fácil de conseguir para gobiernos que suelen violar derechos fundamentales, salvo por una breve lista negra que incluye a Siria o Corea del Norte. Por menos de lo que cuesta un helicóptero militar, un país con pocas competencias técnicas puede comprar un potente sistema de espionaje.

Las redes de espionaje interno dependen de empresas como la israelí-estadunidense Verint Systems, que tiene clientes en más de 180 países. Verint también es proveedora de agencias de seguridad estadunidenses, por ejemplo para perseguir a narcotraficantes en México y Colombia.

El alcance y sofisticación de los productos de Verint quedaron al descubierto en documentos de Perú obtenidos por Associated Press. Se aproximan, aunque en menor escala, a los programas de vigilancia de Estados Unidos y Gran Bretaña descritos en 2013 por el ex contratista de la Agencia de Seguridad Nacional Edward Snowden. Esa información mostró cómo el gobierno estadunidense recopilaba registros telefónicos de millones de estadunidenses, pocos de ellos sospechosos de haber cometido delito alguno.

La documentación incluye manuales de capacitación, contratos, *emails* y recibos, y ofrece detalles hasta ahora desconocidos sobre una industria muy reservada. Verint y otras empresas similares proporcionan poca información sobre sus productos de espionaje y sus compradores.

En Perú, la agencia de espionaje interno del país se gastó apenas 22 millones de dólares en un paquete de Verint apenas unos meses antes de que sus actividades

se vieran frenadas en seco por un escándalo de espionaje interno. Ap confirmó de manera independiente ventas de estos productos en países como Australia, Brasil, México y Colombia.

“El *status* quo es totalmente inaceptable”, dijo Marietje Schaake, una legisladora de la Unión Europea que propugna por una mayor supervisión. “El hecho de que este mercado prácticamente no se regule es muy inquietante”.

Alrededor de la mitad de los acuerdos de vigilancia de Verint están en países en desarrollo, según estimaciones de analistas. Desde principios de la década de 2000, Verint y su principal competidor, Nice Systems, han vendido productos de espionaje masivo a la policía secreta de Uzbekistán y a Kazajistán, según Privacy International, un grupo activista con sede en Londres.

El equipo ha permitido que la policía secreta de Uzbekistán ubique y arreste con rapidez a personas que discuten información sensible por teléfono o *email*, indican disidentes.

“La principal arma de las autoridades es el temor de la gente”, dijo Tulkin Karayev, un exiliado que vive en Suecia. “La libertad de discurso, libertad de expresión… todo está prohibido”.

Al preguntar Ap si las ventas de Nice Systemas habían facilitado la represión política, la vocera de Elbit, que compró la compañía el año pasado, declinó hacer comentarios. “Seguimos las normas que rigen el manejo de las empresas y nos enfocamos en un comportamiento ético para nuestros acuerdos comerciales”, señaló Dalia Rosen.

Las instalaciones de espionaje son un buen negocio, que requieren actualizaciones constantes para seguir el ritmo de las últimas tecnologías. Y pueden sobrevivir a los gobiernos con facilidad.

Por ejemplo, en la nación caribeña de Trinidad y Tobago, el gobierno cayó tras un escándalo de escuchas que incluía equipo proporcionado por Verint. En 2009, un total de 53 personas, entre ellos políticos y periodistas, fueron monitoreadas de forma ilegal. El equipo de Verint aún funciona, aunque ahora se requiere una orden de la corte para utilizarlo.

Como ocurre ahora en Trinidad y Tobago, la mayoría de los países requieren la

firma de un juez para emplear esta tecnología. Pero donde el estado de derecho es débil, los abusos no son inusuales.

Un aparente cliente de *spyware* es el gobierno de Sudán del Sur, donde han muerto decenas de miles de personas en dos años y medio de guerra civil. La Organización Naciones Unidas (ONU) y grupos humanitarios han acusado al gobierno de utilizar herramientas de espionaje israelíes para buscar, encarcelar y torturar a disidentes y periodistas.

Los expertos de la ONU que señalaron a Israel como origen del *software* no identificaron al proveedor del sistema, y un portavoz del gobierno rechazó comentar el tema, aunque un reportero de la Ap confirmó haber identificado a dos empleados de la compañía en un vuelo en mayo de Etiopia a la capital sursudanesa de Yuba. Activistas defensores de los derechos humanos afirman que la vigilancia en el país ha fomentado un clima de miedo y autocensura.

Mínima regulación internacional

La poca regulación que existe en la industria del espionaje masivo se reduce a un régimen internacional de control de exportación de armas no obligatorio llamado el Arreglo de Wassenaar. En diciembre de 2013 fue modificado para agregar productos de vigilancia y espionaje, que se infiltran en dispositivos digitales convirtiéndolos en puntos de escucha. Estados Unidos aún no ha ratificado la enmienda, aunque la Unión Europea sí.

Las víctimas de estas herramientas de espionaje dijeron que les habían mostrado sus correos electrónicos y conversaciones interceptadas.

Joseph Bakosoro, un ex gobernador estatal de Sudán del Sur que también fue detenido sin cargos durante cuatro meses, dijo que sus interrogadores le reprodujeron un mensaje de voz que habían dejado en su celular. Afirmaron que era evidencia de que respaldaba a rebeldes.

Bakosoro dijo que el mensaje de voz sólo demostraba que su teléfono estaba intervenido.

“Dijeron que me monitorean”, dijo. “Monitorean mi teléfono y monitorean a todos, así que cualquier cosa que digamos por teléfono, la monitorean”.

Fuente: http://www.jornada.unam.mx/ultimas/2016/08/02/gobiernos-adquieren-software-para-espiar-a-sus-ciudadanos

Fotografía: jornada.unam

Fecha de creación
2016/08/02