Herramientas baratas permiten espiar a cualquiera

Por FRANK BAJAK y JACK GILLUM
Associated Press, 2 de agosto de 2016

LIMA, Perú (AP) — Fue un escándalo nacional: la entonces vicepresidenta de Perú acusó a dos agentes de inteligencia doméstica de vigilarla. Luego, un importante congresista culpó a la agencia de espionaje de haber forzado la entrada a su oficina. Las historias en la prensa mostraban que la agencia había recopilado información sobre cientos de peruanos influyentes.

Sin embargo, tras el escándalo del año pasado, que forzó la destitución del presidente del Consejo de Ministros y congeló las labores de inteligencia de la agencia, el servicio de espionaje continuó con un programa de 22 millones de dólares capaz de espiar a miles de peruanos a la vez. Perú, uno de los principales productores de cocaína, se unió a la lista de gobiernos en el mundo que han agregado spyware comercial a su arsenal.

La compra hecha a la compañía israelí-estadounidense, Verint Systems, registrada en documentos obtenidos por The Associated Press, permite dar un vistazo inédito tras bambalinas a lo fácil que es para un país comprar e instalar el equipo de espionaje. El software permite que gobiernos intercepten llamadas de voz, mensajes de texto y correos electrónicos.

A excepción de países en la lista negra como Siria y Corea del Norte, se puede hacer poco para impedir que gobiernos que de forma constante infringen los derechos básicos obtengan el mismo equipo conocido como "interceptación legal" que se ha vendido a la policía y agencias de espionaje de Occidente. La gente monitoreada por la tecnología ha sido golpeada, encarcelada y torturada, de acuerdo con grupos defensores de derechos humanos.

Los objetivos identificados por AP incluyen a un bloguero en la represiva república asiática de Uzbekistán, activistas de oposición en el atribulado país africano de Sudán del Sur, y políticos y reporteros en Trinidad y Tobago, en el Caribe.

"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".

Los documentos de Verint que AP obtuvo en Perú, incluidos manuales de capacitación, contratos, emails y recibos, ofrecen detalles hasta ahora desconocidos sobre una industria muy reservada.

"Hay muy poca información confiable sobre esto", dijo Edin Omanovic, un investigador de Privacy International, un grupo activista con sede en Londres. "Estas herramientas comerciales son utilizadas de una forma estratégica y ofensiva muy similar a como se utilizan herramientas militares".

El alcance y sofisticación revelados en los documentos de Perú se aproximan, aunque en menor escala, a los programas de vigilancia de Estados Unidos y Gran Bretaña descritos en el 2013 por el ex contratista de la Agencia de Seguridad Nacional, Edward Snowden. Esa información mostró cómo el gobierno estadounidense recopilaba registros telefónicos de millones de estadounidenses, pocos de ellos sospechosos de cometer crímenes. Incluso después de algunas reformas, falta mucho por hacerse en Estados Unidos y en el extranjero para controlar al Gran Hermano, dijeron defensores de la privacidad.

En las oficinas centrales de Verint en Melville, Nueva York, la asistente del director general, Dan Bodner, dijo que la compañía no haría comentarios. "En general no hacemos comentarios a la prensa", dijo Barbara Costa.

Verint y sus principales competidores vienen de países con agencias de espionaje bien financiadas, como Estados Unidos, Israel, Gran Bretaña y Alemania, y han operado con supervisión limitada.

Con más de 1.000 millones de dólares en ventas, Verint es un viejo participante en una industria cuya discreción hace que sea difícil dimensionar su tamaño. Verint Systems Ltd., el subsidiario que vendió el paquete de vigilancia a Perú, está afincado en Herzliya, Israel, en las afueras de Tel Aviv.

En documentados presentados ante dependencias reguladoras, la compañía dice tener más de 10.000 clientes en más de 180 países, incluidas la mayoría de las compañías más grandes del mundo y agencias del orden público de Estados Unidos. La compañía dice que sus productos ayudan a que los comercios funcionen mejor y "hace que el mundo sea un lugar seguro". En 2007, Verint proporcionó a México una plataforma de vigilancia financiada por Estados Unidos con un valor de 3 millones de dólares cuyo objetivo era luchar contra los cárteles de drogas.

Las ventas de material de espionaje representan cerca de una tercera parte de sus ventas. Sin embargo, la compañía revela poco sobre esos productos, los cuales —dice— recolectan y analizan grandes cantidades de información para "detectar, investigar y neutralizar amenazas".

Tampoco identifica a sus clientes en el sector de seguridad pública y agencias de inteligencia, pero de forma independiente, AP confirmó a través de entrevistas y documentos que tiene ventas en países como Australia, Brasil, Estados Unidos, México, Colombia y Suiza.

Alrededor de la mitad de los acuerdos de vigilancia de Verint están en países en desarrollo, dijo el analista Jeff Kessler, de Imperial Capital, en Nueva York.

La instalación en Perú, conocida como Pisco en homenaje al brandy nacional, demuestra cómo la industria privada de espionaje se ha beneficiado de la multimillonaria inversión que realizan gobiernos de Occidente en vigilancia. Muchos

expertos en seguridad que han perfeccionado sus habilidades en el ejército israelí se han ido a trabajar al sector privado, y con ello han puesto sus talentos tecnológicos al servicio de países menos sofisticados por una fracción del costo.

Al igual que las herramientas de espionaje utilizadas por países más grandes, Pisco le permite a funcionarios "interceptar y monitorear" redes satelitales que llevan tráfico de datos y voz, lo que, de forma potencial, pone en riesgos las comunicaciones privadas de millones de peruanos.

Un manual de software ofrece instrucciones paso a paso sobre cómo interceptar esas comunicaciones con el equipo de Verint: conectarse a un satélite, identificar a la persona que llama, luego "abrir un producto de voz"; su argot para una llamada telefónica.

Lo que sigue en el diagrama de flujo: "Se escucha la voz".

___

"IDENTIFICA NUEVOS OBJETOS DE INTERÉS"

Desde principios de la década del 2000, Verint y su principal competidor, Nice Systems, han vendido productos de vigilancia masiva a la policía secreta en Uzbekistán, según una amplia investigación de Mari Bastashevski para Privacy International. De acuerdo con la pesquisa, las compañías también vendían dichos sistemas al vecino Kazajistán.

Los técnicos israelíes de ambas compañías han entrado y salido de Taskent, la capital de Uzbekistán, para ofrecer apoyo técnico y mantenimiento, halló Bastashevski. Nice Systems vendió el año pasado su división de espionaje a Elbit Systems, una importante compañía israelí de defensa.

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, Dalia Rosen, dijo: "Seguimos los estándares líderes de la gobernanza corporativa y nos enfocamos en el comportamiento ético para nuestros acuerdos comerciales".

En las últimas dos décadas, Uzbekistán ha "encarcelado a miles para imponer un gobierno represor", reportó el año pasado Human Rights Watch. El precio de la disidencia es la detención arbitraria, trabajos forzados y tortura, dijo el grupo. Un

reporte presentado por tres grupos de derechos humanos a la ONU calificó la tortura por parte de la policía secreta de "sistemática, impune y motivada".

Hace tres años, el trabajador metalúrgico Kudrat Rasulov se puso en contacto con Karayev de Uzbekistán vía Facebook para pedir consejo sobre cómo podría promover la libertad de expresión en su país. El exiliado dijo que sugirió a Rasulov, ahora de 46 años, escribir un comentario crítico de la prensa local. Los reportes semanales de Rasulov fueron publicados en internet con un seudónimo. Rasulov pensó que era cuidadoso. Creó una nueva cuenta de correo electrónico para cada artículo que enviaba y luego los dos hombres discutían los artículos a través de Skype. Pero tras seis meses, Rasulov fue arrestado. Ahora cumple con una sentencia de ocho años en prisión por subversión.

Karayev cree que Rasulov fue descubierto mediante vigilancia y Human Rights Watch coincidió con esto. La sentencia de la corte señaló que, en parte, fue declarado culpable por sus comunicaciones vía Skype y su contacto con Karayev, dijo el grupo en su reporte.

"Ellos leían el Skype. Escuchaban sus llamadas telefónicas. Así es como justifican sus acusaciones", dijo Steve Swerdlow, autor del reporte.

En Colombia, Verint ha recaudado millones en ventas. Apenas en 2015, funcionarios de inmigración de Estados Unidos financiaron el mantenimiento para un sistema de intervención telefónica, según los contratos gubernamentales. Hace casi una década, sus productos fueron usados de manera indebida por funcionarios que después fueron despedidos por espionaje ilegal, le dijeron a la AP en ese momento altos funcionarios de la policía y fiscales, quienes hablaron bajo condición de anonimato porque no estaban autorizados para hablar públicamente sobre el tema.

Al igual que en Estados Unidos, la mayoría de los países necesitan órdenes de la corte para utilizar la tecnología. Pero en donde la ley es débil, el abuso no es raro.

El gobierno del país caribeño de Trinidad y Tobago cayó luego del escándalo de intervención telefónica que incluía equipo proporcionado por Verint. En 2009, un total de 53 personas, entre ellos políticos y periodistas, fueron monitoreadas de forma ilegal, según un exfuncionario de seguridad que pidió no ser identificado por temor a represalias. El equipo de Verint aún funciona, aunque ahora se requiere una orden de la corte para utilizarlo.

Uno de los productos de Verint que Trinidad y Tobago compró es Vantage Broadway. Un folleto promocional publicado por el Ministerio de Defensa de Israel para una exposición comercial del 2014 en India lo describe como un software de análisis de información y de búsqueda de patrones. Se enlaza con un producto llamado Reliant para "interceptar, filtrar y analizar enormes volúmenes de comunicación vía internet, voz y satélite". El paquete que Perú compró incluye tanto a Reliant como a Vantage, según muestran documentos.

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 espionaje, como Reliant y Vantage, y "attack-ware", que infiltra smartphones y computadoras convirtiéndolos en puntos de escucha.

Estados Unidos no ha ratificado la modificación: el Departamento de Comercio federal propuso normas que causaron objeción en Silicon Valley. Israel dice que lo acata y la Unión Europea ratificó la enmienda. Pero Schaake, la legisladora de la UE, dijo que sus 28 países miembro actúan de forma independiente y "las tecnologías siguen siendo exportadas a países que son conocidos por violar los derechos humanos".

Mientras tanto, la tecnología de vigilancia de Israel se utiliza en Sudán del Sur, en donde una guerra civil que lleva dos años y medio ha cobrado la vida de decenas de miles de personas, reportó un panel de expertos de la ONU en enero. La ONU y grupos defensores de derechos humanos dicen que el gobierno la utiliza para ubicar, encarcelar y torturar a disidentes y periodistas.

La habilidad de la agencia de Sudán del Sur de "identificar y detener ilegalmente a individuos ha sido mejorada de forma significativa" con la adquisición de "equipo adicional de intercepción de comunicación de Israel", escribieron expertos de la ONU.

No se dio a conocer el nombre de los proveedores, y el vocero del gobierno se negó a discutir el tema. Aunque no hay evidencia directa de que Verint sea proveedor, 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. Mientras escribía en una laptop, uno de ellos trabajaba en una presentación que nombraba a tres empresas de telecomunicaciones que operan en el país.

Verint no respondió a la AP sobre si proveía de tecnología de espionaje a Sudán del Sur.

Un activista encarcelado durante cuatro meses en Yuba dijo que sus interrogadores hablaron abiertamente sobre haber interferido su teléfono, le reprodujeron grabaciones de él en conversaciones intervenidas y le mostraron emails que él había enviado. Habló con la AP bajo condición de anonimato porque dijo temer por su vida.

Joseph Bakosoro, un exgobernador 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 había sido interferido.

Sus interrogadores no ocultaron eso.

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

___

"¿QUIÉN VIGILA A LOS VIGILANTES?"

Tres años después de que Perú adquiriera el paquete Verint, el sistema está instalado pero aún no funciona, aseveró Carlos Basombrio, el nuevo ministro de Interior, que tomó posesión del cargo la semana pasada. "Cuando se operativice, va a ser trabajando con jueces y fiscales en el uso contra crimen organizado".

Ubicado en un edificio de tres niveles a un lado de la agencia de espionaje del país (DINI), Pisco está sobre una base militar en Lima fuera del alcance del público. Puede rastrear a 5.000 objetivos individuales y, de forma simultánea, grabar comunicaciones de 300 personas, según documentos de la agencia, con ocho salas de escucha y una antena parabólica instalada en el exterior para los enlaces satelitales.

El control de Pisco fue transferido a la policía nacional luego del escándalo de espionaje que puso en jaque a la agencia de inteligencia. Verint envió a empleados de Israel para impartir entrenamiento adicional a operadores peruanos, después que el cliente solicitara ocho meses adicionales de capacitación, según registros.

Sin embargo, una importante herramienta de espionaje ha estado activa en Perú desde octubre. Ésta puede rastrear físicamente cualquier teléfono en tiempo real utilizando geolocalización. Según un decreto gubernamental de julio de 2015, la policía puede ubicar teléfonos sin orden judicial, pero necesitaría una para escuchar.

Funcionarios del gobierno no ofrecieron detalles sobre qué software se utiliza para rastrear teléfonos, pero dos meses antes, funcionarios de la DINI autorizaron un pago para un producto de geolocalización de Verint llamado SkyLock. Ese software permite el rastreo de teléfono dentro del país, mientras que una versión superior puede ubicar cualquier teléfono móvil en la mayoría de los países.

Las cuatro compañías telefónicas peruanas acordaron cooperar con la geolocalización al firmar un pacto con el gobierno del cual no se revelaron detalles.

Defensores de las libertades civiles consideran que la geolocalización sin orden judicial es una invasión peligrosa a la privacidad, sobre todo en un país con una alta corrupción pública. El congreso entrante en Perú está dominado por Fuerza Popular, un partido relacionado con el encarcelado expresidente Alberto Fujimori, quien dirigió uno de los regímenes más corruptos en la historia reciente de Latinoamérica.

En julio de 2015, la plataforma de vigilancia Verint se vio enredada en el caos de la política peruana.

Se filtró su compra, lo que ocasionó una auditoría del gobierno. El vicepresidente de Verint en Miami que hizo la venta, Shefi Paz, se quejó de los aparentes retrasos de las empresas de telecomunicaciones en correos electrónicos y cartas dirigidas a funcionarios de la DINI. No se ofrecieron para sostener reuniones.

"Verint no tiene que sufrir por demoras políticas", escribió Paz. Al ser contactado por teléfono, Paz se negó a comentar.

Los productos de espionaje de Verint y sus homólogos juegan un papel importante en la lucha contra el terrorismo, dijo Ika Balzam, un exempleado tanto de Verint como de Nice. Es una afirmación común en la industria y en la cual coinciden los políticos.

Y sin embargo, Balzam reconoció que no hay garantías de que los Estados-nación no abusarán de las herramientas de vigilancia.

"Hay un dicho", dijo Balzam, "¿Quién vigilará a los vigilantes?".

___

El periodista de Associated Press Frank Bajak reportó desde Lima y el periodista de AP Jack Gillum reportó desde Washington. Los periodistas de AP Maria Danilova en Washington; Josef Federman en Jerusalén; Jason Patinkin en Yuba, Sudán del Sur; Tony Fraser en Puerto de España, Trinidad y Tobago; Jamey Keaten en Ginebra y Kristen Gelineau en Sydney contribuyeron a este despacho.

___

Frank Bajak está en Twitter como: https://twitter.com/fbajak

Jack Gillum están en Twitter como: https://twitter.com/jackgillum

___