MUNDO / POLÍTICA

EEUU: La NSA seguirá espiando aún con acceso restringido

El Ciudadano · 18 de junio de 2015

La Agencia de Seguridad Nacional estadounidense (NSA, por sus siglas en inglés) perdió la autoridad con la que apropiarse de los registros telefónicos de millones de americanos a consecuencia del cambio sobre la legislación promulgada después del 11S aprobado la semana pasada. Pero, de todos modos, **no existen pruebas de que el Gobierno realmente haya podido producir inteligencia útil gracias a esos datos** durante los 13 años en los cuales disfrutaban del acceso.

Además, **la NSA sigue aumentando su arsenal de herramientas de vigilancia por internet en suelo americano.** *The New York Times* informó el pasado miércoles de que la administración Obama permite que la NSA intervenga en el cableado de internet dentro del territorio nacional en busca de datos provenientes de intrusiones informáticas realizadas desde el extranjero y de que la agencia no necesita de una orden judicial para hacerlo.

La semana pasada, **la nueva Ley de Libertades Americanas paró en seco la colección en masa de metadatos telefónicos por parte de la NSA –**

registros de cuándo se realizaron llamadas además de sus participantes – y en su lugar requiere que las compañías telefónicas guarden estos datos durante dos años. A partir de ahora, si la NSA o cualquier otra agencia quiere acceder a estos datos, tendrá que solicitárselos a un juzgado federal llamado el Tribunal de Inteligencia Exterior de Vigilancia (también conocido como el juzgado FISA por sus siglas en inglés).

Estos cambios se produjeron mediante una medida que fue aprobada por el congreso el pasado martes y firmada por el Presidente Obama el martes por la noche, un año después de su promesa de reformar este programa (ver *Obama promete una reforma del programa de vigilancia telefónica*). El alcance de la colección de la NSA de registros de llamadas domésticas f**ue una de las revelaciones más significativas de las filtraciones hechas por el contratista de inteligencia Edward Snowden en 2013.**

«Está claro que, hasta cierto punto, esto ralentizará a la NSA», dice un instructor de la clínica legal de la escuela de Derecho de Harvard University (EEUU), Vivek Krishnamurthy. «En vez de recibir todos estos datos masivos que podían utilizar, cortar, y básicamente emplear del modo que quisieran, **tendrán que realizar solicitudes expresas** para obtener datos específicos y concretos cuando se necesiten para el avance de una investigación».

Un informe del comité de privacidad y libertades civiles de la Casa Blanca, conocido como PCLOB (por sus siglas en inglés), concluyó que el valor de la recolección de datos – que empezó después de los ataques terroristas del 11 de septiembre – residía en **poder vigilar y conocer las actividades de terroristas ya identificados con anterioridad** por el Gobierno. Tales conocimientos también se podrían obtener mediante órdenes judiciales al efecto. La recolección en masa no llevó al descubrimiento de ningún terrorista ni ataque del que no se tuviera ya constancia, según las conclusiones publicadas en el informe.

Se avecina otra serie de batallas acerca de cómo el Gobierno debe acceder a los datos. Estas se centran en **cómo las empresas encriptan el correo electrónico y otros datos** de los usuarios y si deben, o no, los cuerpos de seguridad acceder a estos datos encriptados cuando exista una autorización legal para ello.

En parte en respuesta a las revelaciones de Snowden, muchos de los gigantes de la industria de las telecomunicaciones e internet **están implementando fuertes sistemas de encriptación**. Con una frecuencia que va en aumento, empresas como Google y Yahoo encriptan los datos según se desplazan por sus servicios y están dotando a los usuarios con herramientas para que puedan hacer lo mismo (ver*Encriptar los correos dificulta el espionaje* y también *Cómo encriptar tuits, e-mails y estados de Facebook de forma sencilla*). Y Apple ha creado sistemas que encriptan los datos del iPhone de forma instantánea.

El gobierno estadounidense dice que esta tendencia podría entorpecer las investigaciones legales. **El Gobierno ahora quiere que se crean «puertas traseras»**para asegurar el acceso por parte de los investigadores a los datos durante investigaciones criminales cuando los cuerpos de seguridad han obtenido una orden judicial para inspeccionar las comunicaciones de cierto individuo (ver *La Casa Blanca quiere saltarse el cifrado para acceder a datos privados*).

Pero los expertos en seguridad dicen que cualquier sistema diseñado para permitir al paso a agencias gubernamentales estadounidenses podría, en teoría, ser aprovechado por otros. Este anuncio de nuevas escuchas en el cableado nacional de internet seguramente intensifique este debate.

por David Talbot en technologyreview.es Traducido por Teresa Woods
Fuente: **Matrizur / visto en Rebelión**

Fuente: El Ciudadano