CON MALETINES Y SATÉLITES...

El autor de «Diario de un espía» explica cómo los americanos interceptan nuestras llamadas desde Inglaterra. «Por teléfono aún se cuentan muchas cosas»

DAVID R. VIDAL

El coronel del CNI —llamémosle Ramiro— me había pedido que las personas a mi cargo en Marruecos proporcionasen al Centro el mayor número posible de móviles relacionados con «personas de interés». Nada extenso: una simple lista de números de teléfono, anotando a lo sumo el nombre o apodo del usuario. La petición, hasta entonces inusual —mediados de 2005— la justificó porque ya se podía operar sin problemas. Ramiro añadió que debido a la portabilidad de los equipos de escucha —los *maletines*—, los agentes desplegados en Rabat y Casablanca podrían escuchar conversaciones desde cualquier lugar tranquilo: furgonetas, establecimientos tapadera o habitaciones de hotel.

El servicio de inteligencia español precisa de un juez para poder interceptar un móvil en Algeciras. Pero a unas pocas millas de distancia, ya en Tánger, tiene barra libre. Es lo que se llama actuar «en marco de la legalidad»: dentro de las fronteras nacionales existe un procedimiento y de puertas a fuera, otro bien diferente. Obviamente, espías y espiados no tienen la misma percepción de legalidad según el papel que les toque jugar.

El modelo norteamericano es muy similar. Agencias como la CIA. y la NSA han nacido para espiar al resto del mundo. La CIA recibe su poder de su extensa red de informantes, mientras que la NSA hace lo propio con medios técnicos para el espionaje de las comunicaciones, sobre todo las exteriores. Los primeros son más de usar micrófonos y maletines, mientras que los segundos mantienen las distancias y utilizan pantallas de ordenador.

Creer que un servicio de inteligencia puede interceptar las comunicaciones de un líder extranjero y no va a hacerlo raya en la utopía. Si no lo hacen todos es porque no tienen capacidad. Todos los servicios de inteligencia son plenamente conscientes de cuáles son las capacidades de otros servicios y, por extensión, lo son sus gobernantes. El espionaje electrónico no se puede considerar un secreto cuando una de las herramientas más populares, la red Echelon, cuya estación más cercana está en Menwith Hill (Reino Unido), funciona desde los 50. Con ella nos espía la NSA.

Entre espías no está bien visto preguntar cómo se consiguen determinadas informaciones. Sin embargo, en el reparto de cromos entre agencias a nadie le cabe duda de que se ha violado la privacidad de muchos ciudadanos. Las recientes revelaciones de Snowden sólo tienen trascendencia por los efectos que causen en la opinión pública.

El espionaje de la NSA está apoyado con grandes medios, desde aviones a estaciones terrestres. Pero ocupan un destacado papel los satélites. De ahí que la red Echelon se encuentre bajo un control norteamericano de facto. La evolución tecnológica ha permitido que se capten señales cada vez más débiles por lo que el espionaje no se limita al espectro electromagnético más inmediato, como las comunicaciones inalámbricas (teléfonos, radios, satélites…) sino que abarca todo tipo de transmisiones (pulsos en fibra óptica, por ejemplo).

Adicionalmente, la NSA recibe directamente información de las operadoras de telefonía especialmente cuando se trata de llamadas internacionales, *emails* y acceso a datos donde uno de los interlocutores se halla en el extranjero. Esto es así porque la ley conmina a todas las empresas norteamericanas a colaborar. Una copia de todo dato que pasa por sus sistemas es automáticamente reenviado a los servidores de la NSA, donde se encargan de descifrarlo y procesarlo. Esta actividad se complementa con programas como PRISM,que les permite un acceso directo a las cuentas de los usuarios de Google y Yahoo.

Hay que distinguir entre dos tipos de espionaje. Uno de ellos se refiere a los *metadatos*: una especie de registro que incluye el quién, dónde y cuándo de las comunicaciones, pero no el contenido de las conversaciones. En teoría, sólo se iría más allá cuando existan razones específicas y con autorización judicial. La NSA tiene sistemas automatizados que siguen la máxima de grabarlo todo y luego desechar lo que no sirve, por lo que es natural hablar de cifras elevadas. Es el caso de los 60 millones de llamadas que la NSA espió en España en un sólo mes, como reveló EL MUNDO.

El otro tipo de espionaje, que busca interceptar conversaciones de gobernantes como Rajoy o Merkel, se realiza a la antigua usanza. mediante satélites, maletines u otros dispositivos gestionados por agentes de campo. La única restricción es que la operación no se realice en territorio norteamericano.

Uno de los maletines usados para interceptar las comunicaciones.

SE PUEDE CONSTRUIR UN MALETÍN DE ESPIONAJE CON 1.000 EUROS Y HERRAMIENTAS DE DOMINIO PÚBLICO

Recoger una gran cantidad de datos no implica que vayan a utilizarse. Es frecuente que la mayoría de estos acaben en cajones. Como anécdota recuerdo una información recabada en el extranjero mediante un pequeño programa informático, un *troyano*, que no fue transmitida a quienes podrían explotarla porque despertaría sospechas sobre cómo se había obtenido. En inteligencia, no sólo se deben proteger las fuentes, sino también los métodos.

Todo este despliegue tecnológico, que funciona muy bien con políticos y empresas, tiene sus sombras cuando se aplica a aquellos para los que se supone que fue diseñado: los terroristas. El icono del mal, Osama Bin Laden, consciente de las actividades de la NSA, carecía de internet o teléfono, lo que le permitió evadir a las agencias durante años. Aunque en el desierto de Mali una organización terrorista puede enviar un mensaje escrito en un papel portado por un yihadista a lomos de un camello, Bin Laden era mucho más pragmático y usaba la técnica del *sneakernet*: vídeos y mensajes eran llevados físicamente en una memoria USB a un anónimo cibercafé, desde donde se realizaba la transmisión.

APARATO LEGAL, USO ILEGAL

Los *maletines* son una herramienta habitual de los espías ya que, además de ser muy asequibles, permiten realizar escuchas en una zona geográfica muy concreta. Estos maletines son cada vez más famosos tras saltar a los medios tras su presunta utilización por empresas como Interligare en Madrid o Método 3 en Barcelona. En realidad, se pueden adquirir con facilidad: lo ilegal sería su uso, no el aparato en sí. Además, su precio, que hace unos años rondaba los 30.000 euros, se ha reducido sensiblemente. Con pocos conocimientos técnicos y algo más de 1.000 euros es posible construirse uno casero mediante herramientas de dominio público.

¿No se suponía que, al hacerse digital, la telefonía móvil incorporaba el cifrado de las conversaciones para garantizar la privacidad de los usuarios? Sí, pero no la privacidad ante los servicios de inteligencia. Por supuesto, estas barreras no están pensadas para limitar las actividades de agencias como la NSA, que gracias a sus satélites y centros de computación es capaz de descifrar igualmente las conversaciones, sino para otras entidades con menos recursos, dispositivos de escucha portátiles y *hackers* en general.

La aparente torpeza que siempre parece rodear el sector de las telecomunicaciones posiblemente no sea tal, sino consecuencia de ciertos intereses. Puede que sean puramente económicos a la hora de reducir costes en equipos y terminales. O puede que la historia tienda a repetirse: se trata de lograr un sistema lo suficiente seguro ante los *hackers*, pero no tan seguro que complique la vida a los servicios de inteligencia. Y es que por teléfono se siguen contando muchas cosas.

«Diario de un espía», de David R. Vidal, director de GlobalChase, saldrá a la venta próximamente en la Editorial Cúpula Enigmas