Raúl Ornelas Bernal

Un mundo nos espía. El escándalo ECHELON

Fines de 1999. Un escándalo de espionaje entre Estados Unidos y la Unión Europea recordó la existencia de la red de monitoreo de comunicaciones más importante en el mundo: ECHELON. Informes del Parlamento Europeo[1] consignaron la existencia de una vasta red de espionaje dirigida por el estado estadounidense, capaz de analizar cualquier tipo de comunicación en cualquier parte del mundo. ¿De ciencia ficción? Desgraciadamente, no. ECHELON es la expresión acabada de la hegemonía estadounidense y de la muerte progresiva de las democracias occidentales. Un sistema que espía no sólo a los que considera potenciales peligros para la seguridad nacional, sino a sus propios ciudadanos, y que funciona sin ningún tipo de control social, es un peligro enorme para cualquier forma de gobierno mínimamente democrática. En este artículo, queremos presentar sumariamente los rasgos más importantes de este sistema mundial de espionaje.

¿Qué es ECHELON?

Creada en la continuidad de los acuerdos entre Estados Unidos y Gran Bretaña durante la segunda guerra mundial -conocidos bajo el código *UKUSA*-, ECHELON combina diversos servicios de espionaje de Estados Unidos (definido como "socio principal"), Gran Bretaña, Canadá, Australia y Nueva Zelanda (los socios "segundos").[2]

Durante mucho tiempo, la existencia de ECHELON fue mantenida en secreto[3] y sus actividades han sido permanentemente ocultadas. Para ello, se invocaron "razones de seguridad nacional": ECHELON tuvo como objetivo original "vigilar" a los gobiernos del llamado bloque socialista y a los movimientos internacionales considerados "subversivos"

por los gobiernos participantes en el sistema. Sin embargo, el desmoronamiento del "enemigo externo" durante los años noventa implicó un cambio sustancial de la misión encomendada a ECHELON. Durante esa década, sus objetivos no se limitaron a la vigilancia del crimen organizado, de los movimientos revolucionarios, del "terrorismo internacional" y de los países "hostiles" que sobreviven al colapso del Este socialista (Cuba, Libia, Corea del Norte). Progresivamente, el espionaje se extendió hacia el ámbito nacional de los países participantes y hacia el dominio del espionaje comercial.

El relanzamiento de las discusiones sobre ECHELON deriva, precisamente, de diversos asuntos en los que la "información privilegiada" permitió a empresas estadounidenses ganar contratos a sus competidoras europeas. Así, la existencia del espionaje internacional deja de ser un elemento de la "alianza occidental en defensa del mundo libre", para pasar a ser un factor de enfrentamiento entre las potencias dominantes.

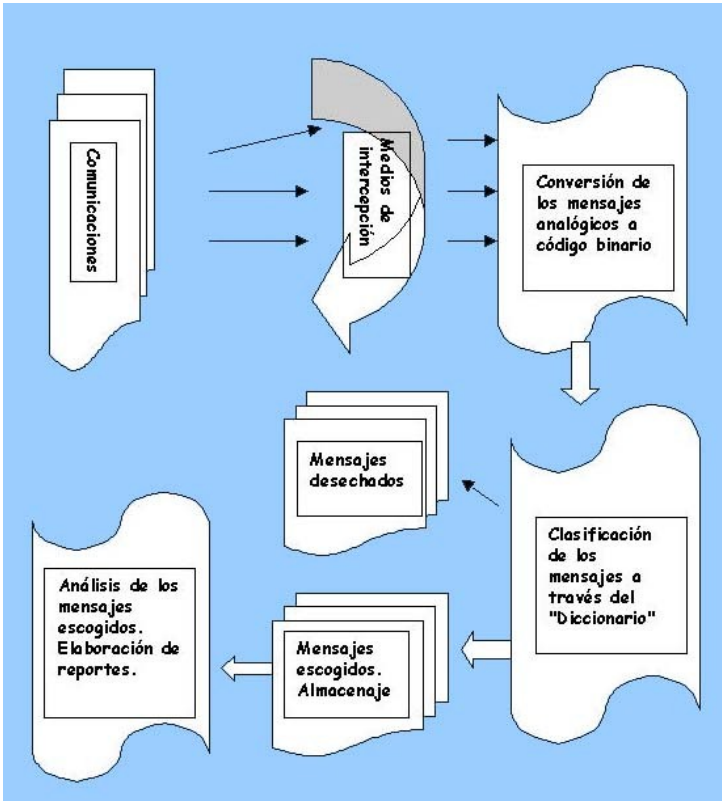
¿Cómo funciona ECHELON?

La cuestión esencial radica en el funcionamiento de este sistema. Una vez definidos los objetivos del espionaje, resulta evidente el carácter titánico de la tarea encomendada a ECHELON: vigilar *todas* las comunicaciones que se realizan en el mundo. A primera vista, tal tarea parecería imposible y hasta absurda. Primero por la complejidad y las dificultades tecnológicas que implica el diseño de un sistema capaz de interceptar los millones de comunicaciones que se realizan diariamente en el mundo. Segundo, y sobre todo, por las cantidades de información generada, cuyo tratamiento y análisis escaparía a los acelerados tiempos del espionaje. Lo interesante del caso ECHELON es que las tecnologías utilizadas ofrecen la posibilidad de alcanzar *lo esencial* de tan descomunal tarea.

El esquema 1 muestra el funcionamiento del sistema.

En el origen se sitúan todas las formas de comunicación privada: llamadas telefónicas, faxes, señales de radio, correos electrónicos y télex, entre las más comunes. Ellas constituyen la materia espiable por el sistema.

La primera capa de ECHELON consiste en los medios de intercepción que captan las comunicaciones y las transmiten a los centros de tratamiento. Centralmente, ello comprende: las estaciones terrestres, los navíos (barcos y submarinos) espías y los satélites secretos ubicados a gran altura (mayor que la de los satélites civiles). El espionaje en Internet se realiza a través de las dorsales,[4] la mayoría de las cuales está manejada por empresas o instituciones estadounidenses.



Los estudiosos de ECHELON ubican once importantes estaciones terrestres de espionaje, cuyo objetivo principal son las transmisiones de los sistemas satelitales, en particular los sistemas Intelsat e Inmarsat. Otras estaciones terrestres, que operan por lo general en bases militares, se encargan de rastrear las transmisiones radiales de alta frecuencia, ligadas con comunicaciones militares.

La red de satélites espías es controlada totalmente por los servicios estadounidenses. Está dedicada a interceptar las comunicaciones por

microondas, por telefonía celular, electrónicas y radiales. Poole[5] estima que esta red posee al menos veinte satélites participando en las tareas de espionaje.

En cuanto a las capacidades de decriptaje, ECHELON está a la vanguardia. Se dice que el sistema ya logró "romper" el algoritmo de criptaje 2028-bits, que es la "llave de protección" más utilizada por las computadoras.[6]

El siguiente nivel de ECHELON es el primer tratamiento de la información. Una vez interceptados, los mensajes son convertidos (cuando es el caso) en código binario, mediante tecnologías informáticas (reconocimiento de caracteres y de la voz, principalmente). En este nivel, podemos observar que este sistema cuenta con avances tecnológicos aún desconocidos por el gran público. Tal es el caso de los sistemas de reconocimiento de la voz, capaces de convertir en texto las conversaciones telefónicas. ECHELON cuenta incluso con un sistema llamado Voicecast, que puede establecer un patrón de voz y rastrearlo para monitorear todas las llamadas de la persona bajo "observación".

Como se dijo antes, la intercepción da como resultado montos inconmensurables de información. La solución aplicada por el sistema es el establecimiento de principios para discriminar las "escuchas" útiles de las desechables. Ello se concreta en programas informáticos capaces de analizar los documentos buscando ciertos patrones (palabras, nombres, sitios, códigos, numéros de teléfono, etcétera). Los llamados "Diccionarios" o compendios de "palabras clave" constituyen la base de tales programas. En ellos, los diferentes servicios de espionaje incluyen los criterios que deben ser rastreados en los mensajes interceptados. Y así, la cantidad de información por analizar se reduce drásticamente. Sólo los mensajes que contienen un término incluido en el "Diccionario" son

grabados y, en ciertos casos, analizados.[7]

Hasta ese momento, todo el proceso es automatizado: la intercepción, la codificación, la búsqueda a partir de los diccionarios se realizan con dispositivos automáticos, entre los cuales destacan las computadoras de procesamiento masivo. Con los mensajes "escogidos", los analistas de ECHELON elaboran diferentes tipos de reportes: traducción y compilación de las intercepciones, clasificaciones por temas, por personas, etcétera... según el gusto del "cliente".

¿A quién espía ECHELON?

Las tareas de espionaje están claramente delimitadas en el interior de la red. En términos geográficos, las estaciones de la NSA se enfocan al continente americano; las estaciones inglesas lo hacen en Europa, África y Rusia; los australianos ayudan al espionaje en Asia septentrional (Sudeste, Pacífico Sur, Océano Índico); los servicios canadienses captan las transmisiones de Rusia, de América y de Europa del Norte, mientras que los neozelandeses tienen a su cargo el espionaje en el Pacífico Sur. Ello no da sino una idea muy general de la distribución geográfica del espionaje que realiza ECHELON, puesto que existe una gran cantidad de "estaciones" en otros países. Detalle para enaltecer nuestro orgullo nacional, el espionaje de las comunicaciones del satélite Morelos se realiza, presumen los estudiosos, desde la estación de Leitrim, en Canadá.

Como anotamos al principio, los objetivos de ECHELON han sido ampliados a partir de la caída del bloque "socialista". En términos generales, se advierten dos evoluciones fundamentales de este sistema: su privatización, simbolizada por su creciente involucramiento en el espionaje comercial, y el acentuamiento de sus rasgos represivos y de control social.[8] Signo de los tiempos, el aparato de gobierno se autonomiza cada vez más del cuerpo social, de tal suerte que "todo el

mundo" pasa a ser parte del "enemigo externo".

En cuanto al espionaje político, ECHELON tiene un rasgo distintivo muy importante. Su carácter internacional permite "saltarse" las prohibiciones acerca del espionaje contra connacionales. Así, un gobierno participante puede pedir a un servicio extranjero realizar el trabajo sucio y quedar a salvo de los controles parlamentarios o judiciales... mientras los espías involucrados guarden el secreto.

Dos ejemplos. En 1983, Thatcher pidió a los servicios secretos ingleses vigilar a dos miembros de su gabinete; con el fin de evitar eventuales problemas, los ingleses pidieron ayuda a sus colegas canadienses. En 1988, se hace público que el senador estadounidense Thurmond estaba bajo vigilancia de los servicios ingleses, a solicitud de la NSA. Lo particular de este caso es que no había razones evidentes para tal vigilancia. Una investigación de la época estableció que no existía un control sistemático acerca de las decisiones de espionaje.

Otros casos han tenido un claro tinte político, buscando proteger -o arruinar- a personalidades de la "alta" política (Trudeau, primer ministro de Canadá; la princesa Diana de Inglaterra). Y también de seguridad nacional, como la vigilancia contra el diputado estadounidense Barnes, por sus comunicaciones con funcionarios sandinistas. Sin embargo, revelaciones de los años noventa han develado que los objetivos de los superespías son cada vez más peligrosos: en 1992, exagentes británicos declararon al *London Observer* que organizaciones como Amnistía Internacional, Greenpeace y Christian Aid eran monitoreadas sistemáticamente.

Finalmente, el espionaje comercial desnuda el carácter de este sistema mundial de "vigilancia". Lejos no sólo de toda noción de seguridad nacional, sino de cualquier "vínculo nacional", los casos de espionaje

comercial relacionan a ECHELON con las empresas proveedoras del sistema. Ello comprende nombres muy conocidos: IBM, Lockheed, TRW, Hughes, entre las más importantes. Una evidencia de que estas prácticas han sido incorporadas a las instituciones de Estados Unidos es la creación de la Office of Intelligence Liaison, adscrita al Departamento de Comercio.

El espionaje comercial ha afectado principalmente a empresas asiáticas: a NCR en un contrato de satélites con Indonesia; a los fabricantes japoneses de autos, acerca del automóvil no contaminante; espionaje en Japón durante las negociaciones sobre el comercio de autos de lujo; espionaje durante la asamblea de la APEC en Seattle (1997), operación que arrojó, entre otras cosas, importantes contratos para la construcción de obras hidroeléctricas en Vietnam, en favor de políticos del Partido Demócrata. Otro detalle folklórico: los servicios canadienses espiaron a la delegación mexicana durante la negociación del TLC en 1992-93.

Actualmente, ECHELON está en el centro de las disputas entre Estados Unidos y Europa. Ello no sólo porque el espionaje ha favorecido a las empresas estadounidenses, sino también porque en Europa, Inglaterra juega el papel de Caballo de Troya. En efecto, los casos más sonados afectaron a compañías francesas: en uno, McDonnell y Boeing vendieron aviones a Arabia Saudita, desplazando a Airbus (que es un consorcio europeo donde los intereses de Francia son dominantes); en otro, Thomson-CSF fue desplazada por Raytheon en un contrato para crear un sistema de seguridad en la Amazonia brasileña. En razón de la participación de Inglaterra en ECHELON, difícilmente las empresas inglesas serían perjudicadas por el espionaje. También se reporta espionaje de la NSA contra el sistema de correo electrónico de la Unión Europea durante las negociaciones comerciales de 1995.

¿Quién dijo que todo está perdido?

Por supuesto que las perspectivas que abre el escándalo ECHELON son negras. Las nuevas tecnologías vienen a agregarse a las ya de por sí pesadas cadenas de nuestra sociedad capitalista. ECHELON aparece como el método de control "perfecto": secreto, supuestamente infalible, libre de toda intromisión de la sociedad. Y sin embargo, es vulnerable. El movimiento pacifista ha abierto varias brechas en contra de ECHELON a través de "invasiones" a las bases del sistema y denunciando su existencia y sus actividades. Las corrientes bienpensantes en Estados Unidos hacen presión sobre los congresistas para que el tema sea discutido en el Parlamento y se haga menos oculto el funcionamiento de ECHELON (¿será posible?). Los piratas de Internet convocaron a un día de embotellamiento de ECHELON: la idea era enviar mensajes con palabras clave o encriptados para provocar una carga importante e inhabitual en el sistema (ver la página http://www.echelon.wiretapped.com).

Todo se vale. Por nuestra parte, sugerimos el gliglico (a la Cortázar), el regreso al papel y la pluma, y de a tiro, la comunicación directa...

Coyoacán, año 2000

Notas:

[1] Ver STOA, *Development of Surveillance Technology and Risk of Abuse of Economic Information (An Appraisal of Technologies of Political Control)*, Luxemburgo, Parlamento Europeo, mayo de 1999. La página de la ACLU (http://www.aclu.org/echelonwatch/index.html) es un buen punto de partida. Para este artículo, además del texto de Poole que citamos más adelante, nos basamos en dos trabajos de Duncan Campbell: *Interception Capabilities 2000*, publicado por el Parlamento Europeo, y *Somebody's Listening*, publicado en 1988 por New Statesman. Ver también el libro de Nicky Hager, *Secret Power: New Zealand's Role in the International Spy Network*, Craig Potton Publishing, Nelson, Nueva Zelanda, 1996.

[2] Los principales organismos "cooperantes" en ECHELON son la National Security Agency de Estados Unidos, los General Communications Head Quarters de Inglaterra, el Communications Security Establishment de Canadá, el Australian Defense Security Directorate y la General Communications Security Bureau de Nueva Zelanda.

[3] La National Security Agency, principal agencia de espionaje estadounidense y eje de ECHELON, fue creada en 1952 bajo la presidencia Truman, y sólo hasta 1957 el gobierno "reconoció" públicamente su existencia. Sobre ella escribe Poole (*ECHELON: America's Secret Global Surveillance Network*, 1999): "*Headquartered at Fort George Meade, located between Washington D. C. and Baltimore, Maryland, the NSA boasts the most enviable array of intelligence equipment and personnel in the world. The NSA is the largest global employer of mathematicians, featuring the best teams of codemakers and codebreakers ever assembled. The latter's job is to crack the encryption codes of foreign and domestic electronic communications, forwarding the revealed messages to their enormous team of skilled linguists to review and analyze the messages in over 100 languages. The NSA is also responsible for creating the encryption codes that protect the US government's communications*".

[4] Las dorsales se componen de las líneas que forman el esqueleto fundamental de las comunicaciones de Internet y de los *routeadores* que organizan el tráfico de datos.

[5] Op. cit. Véase nota 3.

[6] En 1999, se habló de una posible cooperación entre la NSA y Microsoft, con la idea de "plantar" programas espías en Windows, de entregar los códigos de decriptaje y de reducir la eficacia de los medios de defensa contra el espionaje en las computadoras personales. Se esgrimieron como pruebas de esa cooperación, los problemas de seguridad que presentó el navegador de Microsoft, Internet Explorer, la presencia de personal de la NSA en los equipos de ingenieros de esa empresa, así como el hecho de que el principal comprador de Microsoft es el Pentágono.

[7] "*Processing millions of messages every hour, the ECHELON systems churn away 24 hours a day, seven days a week, looking for targeted keyword series,*

phone and fax numbers, and specified voiceprints. It is important to note that very few messages and phone calls are actually transcribed and recorded by the system. The vast majority are filtered out after they are read or listened to by the system. Only those messages that produce keyword 'hits' are tagged for future analysis. Again, it is not just the ability to collect the electronic signals that gives ECHELON its power; it is the tools and technology that are able to whittle down the messages to only those that are important to the intelligence agencies." (Poole, op. cit.)

[8] Digamos de pasada, que la mayoría de los análisis consultados pretenden que ha habido una "perversión" de los objetivos originales de ECHELON. Para estos análisis, el espionaje contra el "enemigo externo" era (y sigue siendo) legítimo y necesario. Lo que ya no se vale, "y es violatorio de las garantías individuales consagradas por la Constitución de Estados Unidos", es que el espionaje se practique contra los ciudadanos estadounidenses (o europeos en la ocurrencia).