VNIVERSIDAD NACIONAL
AVFNOMA DE
MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

"ESPIONAJE INTERNACIONAL Y SU REGULACIÓN: CASO ECHELON"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
LICENCIADO EN RELACIONES INTERNACIONALES
PRESENTA:

ALBERTO GARCÍA REYES

ASESOR: Lic. Briseyda Piedra Aguirre

MÉXICO, 2005

a mi madre,
blanca reyes maldonado,

a mi padre,
alberto garcía bocanegra

AGRADECIMIENTOS

CCH Vallejo

FES Aragón

Lic. Briseyda Piedra Aguirre

y a toda aquella persona que participó para la elaboración de esta tesis

Índice

INTRODUCCIÓN

INTRODUCCIÓN

Ante los latentes procesos de globalización es frecuente encontrar temas de la agenda internacional relacionados con avances tecnológicos. Es común escuchar en temas como desarme nuclear, terrorismo, economía mundial, medio ambiente cuestiones relacionadas con nuevas tecnologías como computación, internet, satélites etc. es decir, los avances tecnológicos están ligados en cualquier ámbito internacional.

Los avances tecnológicos se involucran de manera amplia en las esferas sociales, económicas, militares, políticas y culturales de todas las naciones, es evidente que estos temas requieren de una tecnología de punta para un mejor desempeño y por supuesto que estos avances requieren de una comprensión clara y concisa para un mejor aprovechamiento. Además de que los avances tecnológicos nos afectan a todos directa o indirectamente, todos requerimos de ellos de una forma u otra, además están implicados en las actividades que desarrollamos a diario, incluso requerimos de ellos para nuestra seguridad; además que los gobiernos los utilizan para combatir cuestiones bélicas.

En las últimas décadas hemos visto que cuando se mencionan conflictos bélicos o programas de defensa, resulta necesario relacionarlos con la tecnología de punta con la cual se cuente. Los satélites señalan en gran parte el destino a seguir en estos acontecimientos debido a su ubicación estratégica por parte de los gobiernos.

Los beneficios que proveen los avances tecnológicos en cuestiones de seguridad y de guerra son infinitos y merecen de nuestra atención. Los gobiernos invierten millones de dólares para poner en órbita satélites que proporcionan todo tipo servicios desde telefonía hasta servicios de seguridad nacional.

Resulta de trascendental importancia comprender la importancia que tienen los avances tecnológicos y su aplicación en las necesidades del ser humano; además de sus implicaciones notorias dentro de las Relaciones Internacionales.

Cabe mencionar que los atentados terroristas que se han originado a principios de este siglo han sido una constante preocupación por parte de los Estados, es cada vez más la inseguridad una inquietud, un problema que aqueja a todos los Estados del orbe. Y es de esperar que EE.UU. como uno de los principales afectados por el terrorismo adopte medidas drásticas en cuanto a su seguridad nacional.

No es posible entender una potencia económica y militar –como EE.UU.- sin un efectivo sistema de seguridad nacional, sobre todo cuando en la actualidad existe una preocupación de inseguridad en todo el mundo. Y es aquí donde Echelon[1] ((la mayor red de espionaje del mundo lidereada por Estados Unidos), a través de sus 120 satélites intercepta todo tipo de comunicaciones que utilizan instrumentos electrónicos y digitales (las comunicaciones telefónicas, los fax y el correo electrónico) en todo el mundo.

La elección de este tema ***Espionaje internacional y su regulación: caso Echelon***, es debido a su gran importancia dentro del ámbito internacional, podríamos decir que es un tema con un gran potencial internacional que merece nuestra atención. Además me parece oportuno exponer un tema que en esencia es nuevo, que su información es fresca, Echelon fue reconocido oficialmente en el año de 1999. Asimismo es un tema diferente y original.

Otro aspecto que me impulsó a elegir este tema fue el gran interés que tengo acerca de temas relacionados con las comunicaciones y con los avances

[1] Echelon significa escalón.

tecnológicos (temas vinculados ampliamente). Asimismo es significativo exponer un tema que es prácticamente desconocido como lo es el espionaje internacional.

Desde que el Sputnik[2] (primer satélite artificial) fue lanzado el 4 de octubre de 1957 por la URSS, seguido por el Explorer 2[3] en enero de 1958, lanzado por Estados Unidos; se inició la era espacial, una era que traería consigo toda una serie de adelantos tecnológicos, pero que también traería una serie de interrogantes concernientes al derecho ultraterrestre[4], a las economías de los países participantes, al adecuado uso de los satélites, a la organización y estructura de los sistemas satelitales de los países participantes.

Debido a que todos somos afectados en mayor o menor medida, directa o indirectamente de los avances tecnológicos su regulación requiere de nuestra atención, demanda la participación de los Estados y de todos los actores internacionales.

En la actualidad algunos países desarrollados cuentan con ciertas redes satelitales y la mayoría son usadas para espiar cuestiones económicas, políticas, bélicas, comerciales, militares etc. Por supuesto todas estas redes representan "cierta seguridad" pero a la vez representan complicaciones legales. Estas complicaciones se acrecientan sobretodo cuando la mayoría de estos países niegan la existencia de sus redes y por lo tanto desconocen las demandas y quejas de las victimas espiadas. Ocasionando así, un panorama de incertidumbre para afrontar tal situación.

---

[2] El *Sputnik 1* era una esfera de aluminio de 58 cm de diámetro y pesaba 83 kg. Tardaba 96,2 minutos en dar la vuelta a la Tierra.
[3] Era una nave cilíndrica de 14 kg, 15 cm de diámetro y 203 cm de longitud, que estuvo transmitiendo mediciones de radiación cósmica y micrometeoritos durante 112 días.
[4] *cfr.* Manfred Lachs, *El derecho ultraterrestre*, p.8

En estos tiempos donde la información es mucho más valiosa que el armamento, es necesario estar informado de todas las maneras posibles. Echelon observa, escucha, intercepta e-mails y faxes. Echelon lleva a cabo espionaje militar, político, civil y comercial, es en este último donde se desprenden un sin numero de acusaciones por parte de las victimas (sobre todo europeas).

Echelon no solo espía cuestiones militares o políticas sino también comerciales. Esta red se involucra en espionaje industrial y en obtener secretos comerciales para beneficiar a una o a muchas compañías norteamericanas. De esta manera, roba secretos comerciales de empresas europeas, es decir, la Comunidad Económica Europea es vigilada por este sistema en un espionaje industrial. Echelon roba a las industrias europeas algunos de sus más valiosos secretos comerciales.

La problemática es que los responsables de crear y operar la red no reconocen su existencia, por lo tanto es difícil enfrentar el problema, tampoco existe un órgano internacional capaz de tomar medidas que enfrenten tal situación y sobre todo que no existen garantías de privacidad y seguridad cuando se efectúa algún tipo de comunicación en el mundo.

La política internacional, al igual que todo tipo de política, es una lucha por el poder[5]. No importa cuales sean los objetivos finales de la política internacional, el poder se constituye invariablemente en el fin inmediato.

El realismo político[6] afirma que el Estado Nación -actor principal de las Relaciones Internacionales- tiene como prioridad principal el poder, la seguridad nacional y la supervivencia del mismo, y para llegar a estos fines el Estado hará uso de amenazas, mandatos, persuasión, autoridad, dotes o mediante una acertada coalición de estos elementos.

[5] Como lo menciona Hans J. Morgenthau en: *De Politics among Nations: The Struggle for Power and Peace.*
[6] Hans J. Morgenthau es conocido como el *padre del realismo político.*

Debido a las exigencias actuales a las que se enfrenta un Estado Nación, como crecimiento, estabilidad, reconocimiento, seguridad etc., no es un secreto que algunos Estados recurran a prácticas que afectan la soberanía y derecho de otros Estados con el fin de conseguir su objetivo.

La seguridad nacional es una de las máximas inquietudes en la actualidad para cualquier Estado; el realismo político admite la búsqueda por la seguridad y la supervivencia del Estado, y que éste se valdrá de todos sus recursos aunque no todos estén dentro de marco legal, ya que existe una anarquía estructural mundial, donde predomina el más poderoso. La conducta del Estado no puede ser reformada, sino sólo controlada.

Un ejemplo claro de uso de poder es EE.UU., hace uso de su tecnología satelital para espiar a cualquier país del mundo, (tomando fotografías, grabando videos, interceptando llamadas telefónicas y correos electrónicos etc.) y de esta manera invade la soberanía, argumentando que sólo se protegen de cualquier situación que perturbe su "orden" como por ejemplo de algún ataque terrorista.

El realismo político acepta que este mundo es imperfecto y que así seguirá ya que existe una baja probabilidad de transformación del sistema. El mecanismo regulador de este mundo internacional sólo puede ser el equilibrio de poder[7], mediante el cual es posible evitar que un Estado pueda imponer su hegemonía. La contraparte del realismo es el idealismo, este se esfuerza por extender la idea de que las naciones deben cooperar estrechamente las unas con las otras para

[7] Henry Alfred Kissinger en 1969 ingresó al gobierno de Richard Nixon como consejero de seguridad nacional, pero luego ocupó el puesto por el cuál se lo recordará siempre: el de secretario de Estado. Fanático del equilibrio del poder, Kissinger ha sido calificado como un "realista" por sobre todas las cosas.

evitar la miseria y los conflictos. Esa cooperación no sólo debe ser política, sino también económica. El idealismo comparte una perspectiva sobre el mundo basada en ciertas creencias: la naturaleza humana es esencialmente altruista y, por lo tanto, las personas son capaces de ayuda mutua y colaboración; el mal comportamiento humano es resultado de instituciones y arreglos estructurales, no proviene de la naturaleza misma de los humanos; por consecuencia, la guerra es evitable ya que es producto de ciertas instituciones que la promueven, las cuales podrían ser eliminadas; la sociedad internacional debería reorganizarse para reconocer la guerra como un problema internacional y eliminar aquellas instituciones que promuevan la guerra, en favor de aquellas que adelanten la paz

En la actualidad el sistema Echelon lleva a cabo sus operaciones de espionaje militar, comercial, político y civil en todo el mundo, sin que exista algún tipo de instrumento jurídico que enfrente tal situación evidenciando así la falta de atención a tal problema.

La hipótesis de este trabajo pretende demostrar que sí no se lleva a cabo la regulación de los sistemas de seguridad nacional o sistemas de espionaje internacional (que para el caso es lo mismo) como Echelon, es indudable que seguirá predominando en el escenario internacional el mismo contexto de intransigencia, anarquía, autoritarismo y absolutismo.

Como respuesta tentativa a la hipótesis resulta difícil pensar en una rápida y efectiva solución al problema, debido al actual contexto internacional agobiado por problemas bélicos, terrorismo, narcotráfico, en donde países como EUA y Gran Bretaña luchan por su seguridad y es aquí donde Echelon es un arma primordial para luchar contra todos estos problemas mencionados.

Por lo tanto la presente investigación tiene como objetivo demostrar con base en demandas, reportes, testimonios, investigaciones y todo tipo de pruebas, que Echelon lleva a cabo sus actividades -intercepta 3 000 millones de comunicaciones al día, incluyendo llamadas telefónicas, fax, mensajes de correo y transmisiones vía satélite- sin apego a un marco legal, es decir, sus actividades violan los derechos de los ciudadanos así como el de los Estados, dañando la vida política, comercial, militar y económica de los Estados espiados; argumentando que todas sus actividades son realizadas en pro de la seguridad nacional sobretodo de Estados Unidos y Gran Bretaña.

La importancia de analizar los antecedentes, conceptos y técnicas del espionaje internacional, radica en que esta actividad ha sido utilizada por los Estados desde antes del siglo XX alterando así el curso de la historia.

En la actualidad existe un gran desconocimiento alrededor de la red de espionaje más poderosa del mundo, así pues, debemos de poner en evidencia la red Echelon, exponer su definición, su funcionamiento, su historia, su estructura, para así darnos cuenta de la magnitud de sistema de la que estamos hablando.

Actualmente no existe algún tipo de autoridad que enfrente a la red de espionaje Echelon, aún a sabiendas que existen estatutos y leyes que protegen la privacidad en las comunicaciones civiles y en las transmisiones de datos. La ausencia de atención a esta situación solamente seguirá manteniendo intransigencia en el contexto internacional pero en pro de países como Estados Unidos y Gran Bretaña.

Es importante realizar las siguientes interrogantes para tener una mejor concepción del tema que se va a tratar:
¿Cuál es la importancia del espionaje internacional en el actual contexto mundial?

¿Cómo está constituido Echelon?
¿Cuál es el papel del Derecho Internacional en Echelon?

El siguiente trabajo de investigación consta de tres capítulos, en el primero se presenta todo lo referente al espionaje internacional como su definición, su historia, sus técnicas. La importancia de este capítulo radica en que el lector apreciará el espionaje como una actividad desconocida pero significativa a lo largo de la historia internacional; además de inmiscuirse en las diferentes formas en las que el espionaje puede ser efectuado, así pues este capítulo pretende ubicar al espionaje como una actividad bien establecida a lo largo de la historia.

El segundo capítulo está enfocado en su totalidad al sistema internacional de espionaje: **Echelon**, este apartado revela información sorprendente y a la vez significativa acerca de la red de espionaje más poderosa del mundo. Los datos de este capítulo pretenden despertar el interés y tal vez la inquietud del lector, ya que todo aquel que utilice los medios electrónicos de comunicación no es ajeno al campo de acción que desarrolla esta red.

En el tercer capítulo y último, se presenta de que manera (si es que existe) el derecho internacional puede enfrentar el accionar del espionaje internacional. El asunto aquí, es saber sí existe algún tipo de instrumento jurídico internacional ya sea un convenio, tratado, o estatuto capaz proteger la privacidad del individuo; además manifestar la privacidad como un derecho fundamental, mostrando su importancia y la necesidad de respetarla dentro de una sociedad bien establecida.

CAPÍTULO 1

DEFINICIÓN, HISTORIA Y TIPOS DE ESPIONAJE

1. Definición, historia y tipos de espionaje

Debido a que el espionaje es una actividad secreta, resulta difícil aseverar sus hechos, solo apoyándose en información seria y prudente (ya que fácilmente podemos caer en exageraciones y/o imprecisiones) podemos informarnos de cuales han sido los escenarios que ha vivido esta actividad a través de los años. El espionaje como cualquier otra actividad de la humanidad, goza de un pasado[8], presente (el cual en gran parte es desconocido) y seguramente un futuro inédito.

Cuando se habla de espionaje surge inmediatamente el concepto de tecnología, se habla de submarinos, satélites y toda clase de mini aparatos como salidos de una película, indicando así a relación espionaje-tecnología. El espionaje necesita irremediablemente de una tecnología de punta para realizar su cometido, es decir, sin una tecnología eficiente y poderosa el espionaje simplemente fracasaría. Es por eso que países y organizaciones invierten millones de dólares anualmente en el desarrollo de nuevas tecnologías, ya sea en el sector militar, científico o en el campo del espionaje.

De esta manera, el espionaje cuenta con antecedentes, infraestructura, sistema, métodos, apoyos, herramientas, y con un conjunto de características que hacen del espionaje internacional la envidia de cualquier otra industria o actividad establecida formalmente en el mundo. El espionaje internacional ha sido y es una actividad tan utilizada como secreta, no existe razón alguna para pensar que esta actividad fuera a desaparecer pronto, lo único que pudiera detener el espionaje es que el hombre dejara de crearlo y de efectuarlo, lo cual resulta poco probable conociendo las ventajas que ofrece ésta actividad.

---

[8] Que por cierto es muy vasto, se tienen registros de espionaje en la Biblia. (Antiguo Testamento, Josué 2, 3, *Rajab y los espias.)*

1.1 Espionaje internacional

El espionaje ha sido y continúa siendo tema de innumerables novelas, películas e incluso videojuegos[9], pero la realidad indica que la mayoría de los casos de espionaje reportados van más allá de una simple novela, película o videojuego.

Cuando un Estado, Organización ó cualquier actor internacional necesita obtener información significativa de otras naciones existen dos métodos: enviar un embajador ó representante y qué averigüe con base a una serie de protocolos, y la otra opción es enviar un espía y que lo averigüe como pueda.[10] Es de todos conocido que las Naciones buscan tener ventajas unas sobre las otras, sin importar que el método para este fin sea precisamente ético ó moral. Cuando se han agotado todos los medios diplomáticos posibles para llegar a un acuerdo o para conseguir algún tipo de información y éstos no han dado los resultados esperados se tiene que pensar en otras alternativas, sí es que se quiere cumplir el objetivo deseado.

Es entonces cuando se tiene que recurrir al espionaje, el cual es llevado a cabo para obtener información de difícil acceso y sobretodo de mucha importancia. Obviamente no cualquier país u organización pueden llevar cabo ésta actividad ya se requiere tecnología, presupuesto, personal capacitado etc.

No existe una definición exacta, la siguiente definición es construida conforme a los documentos consultados a lo largo de esta investigación: el espionaje internacional es la práctica y conjunto de técnicas asociadas a la obtención de información confidencial en el extranjero, es decir, es cuando el

---

[9] Metal Gear Solid y Splinter Cell son videojuegos de espionaje internacional y ambos reportan ventas a nivel mundial.

[10] Hacer uso de sus habilidades para escuchar, observar, merodear, curiosear, informarse disimuladamente sin que despierte sospecha alguna.

espionaje rebasa las fronteras. Sus campos de acción son el espionaje industrial, civil, comercial, político, militar, científico etc.

Una nación podrá efectuar tantas acciones de espionaje como le sea posible. El espionaje internacional es utilizado de diversas maneras, actualmente con los avances tecnológicos es posible desarrollar diferentes técnicas de espionaje que en el pasado hubieran sido imposibles de realizar. En la actualidad podemos encontrar por ejemplo los satélites, el internet, los submarinos que desplazan las antiguas técnicas de espionaje como lo era mandar agentes espía.

1.2 Historia del espionaje internacional

El espionaje nació como consecuencia del secreto, es decir, al mismo tiempo, que el género humano.[11] Los primeros hombres que acorralaban la presa y tendían emboscadas, practicaban el secreto, como los gobiernos que protegen su tecnología de punta y disimulan sus armamentos. Y cada vez que un individuo establece la barrera del secreto, otros individuos, otras naciones intentan perforarla, a veces con una meta de dominio, más a menudo con la defensa por objetivo.

"La antigüedad del espionaje queda atestiguada por numerosos textos; en la Biblia según cuenta la historia los jefes de tribus enviados por Moisés para reconocer el país de Canaán, los agentes de Josué en Jericó, y muchos otros espías menos conocidos, se encuentran ocultos en los repliegues del Antiguo Testamento."[12]

---

[11] Una vez que el ser humano tiene conciencia de lo que es y lo que hace, desarrolla entre otras cosas el espionaje.
[12] Ramón García *Enciclopedia metódica Larousse*. p.749

Josué 2, 3

Rajab y los espias

Luego Josué hijo de Num envió secretamente desde Sitín, a dos espías con la siguiente orden: "Vayan a explorar la tierra, especialmente Jericó". Cuando los espías llegaron a Jericó, se hospedaron en la casa de una prostituta llamada Rajab. Pero el rey de Jericó se enteró de que los espías israelitas habían entrado esa noche en la ciudad para reconocer el país. Así que se le envió a Rajab el siguiente mensaje: "Echa fuera a los hombres que han entrado en tu casa, pues vinieron a espiar nuestro país".[13]

La información pronto fue reconocida como una herramienta vital para el Estado, tanto para la diplomacia como para la guerra. "Hace más de 2500 años el teórico militar chino Sun Tzu subrayó su importancia. En su libro "El Arte de la Guerra"[14] (c. 500 a.C.) daba instrucciones detalladas para organizar un sistema de espionaje con agentes dobles y desertores. El espionaje, sin embargo, estuvo organizado por los gobernantes y los jefes militares hasta la aparición de los nacionalismos, de las fuerzas armadas regulares y de la diplomacia en el siglo XVIII."[15]

[13] Santa Biblia, Sociedad Bíblica Internacional, México, 1999, p.220
[14] Sun Tzu, *El arte de la guerra*, Ed. Gernika, México DF. 1994, 118 p.
[15] Andri Fernez. *El espionaje por dentro*. Traduc. Josi Baeza, p. 14

1.2.1 *En el siglo XIX*

"Se cree que el espionaje político fue empleado por primera vez de forma sistemática por Joseph Fouché, duque de Otranto[16] que fue ministro de Policía durante la Revolución Francesa y el imperio de Napoleón I. Siguiendo las órdenes de Fouché una red de agentes de policía y espías profesionales descubrió una serie de conspiraciones para hacerse con el poder por parte de los jacobinos[17] y de los monárquicos borbónicos exiliados. El príncipe de Metternich[18], estadista austriaco, también creó una eficiente organización de espías políticos y militares al principio del siglo XIX. Más conocida que estas organizaciones fue la temida Ojranka (Servicio de Seguridad) de los zares rusos. Se creó en 1825 para descubrir la oposición al régimen."[19]

A mediados del siglo XIX se reorganizó la policía secreta de Prusia con la misión de proteger la seguridad interna y externa del país. "El sistema de espionaje prusiano jugó un papel clave en los pasos iniciales del proceso de unificación alemana. También se ocupaba de Francia con una red de más de 30 000 agentes cuyo trabajo contribuyó a la victoria alemana en la Guerra Franco-prusiana (1870-1871). Sin embargo, los estados modernos no crearon departamentos permanentes de espionaje hasta la última parte del siglo XIX."[20]

---

[16] Joseph Fouché, duque de Otranto (1758-1820), político francés, conocido como el padre del espionaje político moderno.
[17] Jacobinos, nombre que recibían los miembros del club radical francés que dirigió la vida política del país durante la Revolución Francesa.
[18] Klemens von Metternich, conde y príncipe de Metternich-Winneburg (1773-1859), político y diplomático austriaco, una de las más importantes figuras de la política europea del periodo comprendido entre 1814 y 1848.
[19] Biblioteca de Consulta Microsoft® Encarta® 2003. © 1993-2002 Microsoft Corporation.
[20] *Idem*

1.2.2 *A principios del siglo XX*

El espionaje sistemático ayudó a los japoneses a derrotar a los rusos en la Guerra Ruso-japonesa (1904-1905).[21] Al prepararse para la I Guerra Mundial los alemanes volvieron a inundar Francia con una tropa de agentes camuflados como representantes, profesores, campesinos o criados. Los agentes alemanes también intentaron sabotear la defensa nacional de Estados Unidos antes y después de su entrada en la I Guerra Mundial.[22]

Sin embargo, muchas naciones participaron en esta contienda con servicios de espionaje deficientes, y muchas veces se luchó con información incorrecta. Las lecciones aprendidas en aquella guerra y los rápidos avances de la tecnología (sobre todo en comunicaciones y aviación) provocaron un crecimiento importante de los servicios de inteligencia. Esto se acentuó aún más con la llegada de gobiernos con políticas exteriores expansionistas (los fascistas en Europa y la dictadura militar en Japón) y con la creación de la Gestapo[23] en la Alemania nacionalsocialista. Estos acontecimientos hicieron que otros países democráticos también organizaran sistemas de contraespionaje.

1.2.3 *En la II Guerra Mundial*

La II Guerra Mundial fue el punto definitivo para los servicios de inteligencia en todo el mundo. Las modernas tecnologías militares y de comunicaciones hicieron imprescindible la información precisa y rápida. Algunas de las grandes batallas de esta guerra se entablaron entre los servicios de espionaje y contraespionaje. No hace mucho tiempo han sido revelados algunos de estos

---

[21] La causa de la guerra fue que la expansión rusa en Asia oriental chocó con los planes japoneses de tomar posiciones en el continente asiático.
[22] *cfr* Biblioteca de Consulta Microsoft® Encarta® 2003. © 1993-2002 Microsoft Corporation.
[23] Gestapo (Geheime Staatspolizei o Policía Secreta), apelativo común empleado para referirse a la policía política del régimen nazi.

éxitos, y algunos errores en esta contienda secreta. Entre los éxitos, la Operación *Double Cross* (Cruzada Doble) es notable: los británicos capturaron durante la guerra a casi todos los espías alemanes que actuaban en Gran Bretaña y los convirtieron en agentes dobles que remitían informaciones equívocas y manipuladas a Alemania. Además, los británicos y sus aliados consiguieron descubrir el código secreto alemán, por lo que tuvieron acceso a muchas de las transmisiones secretas del enemigo.[24]

"El ataque por sorpresa de Japón a Pearl Harbor el 7 de diciembre de 1941 supuso un gran éxito de los servicios de inteligencia japoneses y un gran fallo para los estadounidenses. Aquel fallo estimuló el respaldo a la ampliación de un enorme aparato de inteligencia en Estados Unidos después de la guerra. Antes de la II Guerra Mundial, Estados Unidos no tenía en la práctica ningún servicio de inteligencia, pero después de la guerra la CIA[25] adquirió renombre en todo el mundo por su omnipresente vigilancia internacional, uniéndose así al MI6[26], el KGB[27], *al Service de Documentation Extérieure et de Contre-Espionage* de Francia, al Mossad (servicio de inteligencia de Israel) al Departamento de Asuntos Sociales de China y a muchos otros departamentos de inteligencia en una enorme red de espionaje y contraespionaje internacional."[28]

1.2.4 *A finales del siglo XX*

A mediados de la década de 1970, como resultado de la desilusión provocada por la guerra de Vietnam y el escándalo del Watergate y de la política de distensión, muchos estadounidenses empezaron a cuestionar el papel

---

[24] *cfr* Juan Brown. *Esbozo de Historia Universal* p. 215

[25] La CIA (Central Intelligence Agency, Agencia Central de Inteligencia),
es la primera agencia permanente de información responsable de mantener al Gobierno al día de las acciones extranjeras que afecten a los intereses del Estado.

[26] Siglas del Servicio Secreto de Inteligencia británico.

[27] KGB, siglas de Komitet Gosudarstvennoy Bezopasnosti (nombre ruso que, en español, significa Comité de Seguridad del Estado), policía secreta de la Unión de Repúblicas Socialistas Soviéticas (URSS), encargada de defender el régimen comunista soviético contra enemigos internos y externos.

[28] Biblioteca de Consulta Microsoft® Encarta® 2003. © 1993-2002 Microsoft Corporation.

de la CIA. Los medios de comunicación descubrieron abusos y errores de la Agencia, a lo que siguieron investigaciones de comisiones presidenciales y de comités del Congreso. Éstos fijaron una nueva línea para las operaciones secretas y una nueva estructura para su supervisión por parte de los cuerpos ejecutivos y legislativos. Sin embargo aún continúa la polémica sobre el papel de la CIA y sobre su control. Uno de sus resultados es que cada vez hay más información pública sobre los servicios de inteligencia en todo el mundo.

1.3 Técnicas de espionaje

1.3.1 *Las escuchas microfónicas*

La tecnología ha hecho progresos fantásticos en el curso de las últimas décadas; por supuesto, los servicios de información han explotado aquellos que podían tener una aplicación en sus dominios específicos; algunos de sus medios de investigación han sido perfeccionados y han aparecido métodos nuevos.

Se ha dicho que la actualidad esencial del espionaje consiste en ver y oír. Los progresos de la tecnología han permitido ver y oír mejor. Lo que ha hecho posible oír mejor es el desarrollo de los procedimientos de escucha y de registro de los sonidos, especialmente la palabra. Esas intercepciones de los sonidos tienen lugar ya sea directamente, o en el curso de su transmisión por un hilo (teléfono, radiofonía). En todos los casos, se captan los sonidos mediante un *micrófono*, y se les envía a un aparato registrador (*magnetófono*[29]), o bien mediante emisores de radio asociados a los micrófonos, o mediante hilo. Estas técnicas son relativamente antiguas; pero lo que es nuevo, es la aparición de

[29]Aparato que transforma el sonido en impulsos electromagnéticos destinados a imantar un alambre de acero o una cinta recubierta de óxido de hierro que pasa por los polos de un electroimán. Invertido el proceso, se obtiene la reproducción del sonido.

materiales muy complejos –micrófonos y micro emisores miniaturizados, micrófonos de naturaleza particular- que han ofrecido a los servicios de información posibilidades inéditas, han ampliado su arsenal y diversificado sus métodos.

Actualmente es posible fabricar micro emisores del tamaño de una lenteja, que se pueden disimular en una flor, una joya o un diente. Estos aparatos no tienen más que un alcance limitado y no son confiables. Pero si se pasa al tamaño inmediato superior, el de un fríjol, para seguir con las comparaciones vegetales, se obtienen materiales totalmente funcionales. Estos micro emisores son los más utilizados en la "plomería" de los locales, y sobre todo de las embajadas; se disimulan en las habitaciones en que puedan tener lugar conversaciones útiles,[30] pero también cerca de las camas (para eventuales chantajes sexuales), de las cajas fuertes (descubrimiento de las combinaciones), y en las máquinas de escribir (análisis de los sonidos de la máquina y reconstitución de los textos dactilografiados). Estos dispositivos se emplean a gran escala en los países del Este. La "limpieza" de las embajadas occidentales de Moscú, Praga o Sofía ha permitido descubrir, en algunos años, más de 30 micrófonos en un solo edificio.[31]

No siempre es necesario colocar un micrófono en una habitación para captar sonidos. Todas las superficies que vibran bajo las ondas sonoras pueden sustituirlos; las pastillas del teléfono, los altoparlantes de una cadena de alta fidelidad, por ejemplo, pero también los ceniceros, los espejos, los vidrios de las ventanas; estos objetos funcionan como *contestadores pasivos*. Hace una veintena de años, los servicios de seguridad norteamericanos hicieron un extraño descubrimiento en la oficina de su embajador en Moscú. Encima del sillón del diplomático estaba colocado el emblema nacional, una magnífica águila de madera regalada por el entonces gobierno soviético; al examinar de cerca el

[30] En los cuadros, las lámparas, bajo las mesas.
[31] *cfr.* Jean Pierre Alem, *El espionaje y el contraespionaje*, p.51

objeto, los expertos estadounidenses encontraron en uno de los pliegues un diafragma conectado a una corta antena. Es entonces como se identificó el primer *contestador pasivo*. Estos objetos vibran al sonido como los micrófonos, y sus vibraciones modulan un haz electromagnético dirigido hacia ellos; el haz reflejado se capta y su desmodulación permite restituir los sonidos y las conversaciones. Los haces empleados son haces radar o, en el caso de los vidrios, rayos láser. Estos contestadores pasivos presentan numerosas ventajas: no son detectables dado que forman parte del ambiente normal; no comportan alimentación y funcionan por tanto indefinidamente; pero no son seguros; una pipa colocada en un cenicero, una persiana cerrada pueden reducirlos al silencio.[32]

1.3.2 *Señales de Inteligencia*

Las escuchas microfónicas intervienen en las acciones tácticas de los servicios de información. Con las escuchas por radio, que permiten interceptar los mensajes intercontinentales, se pasa al plano estratégico.

Las transmisiones por ondas hertzianas se han desarrollado en proporciones fantásticas desde la puesta en servicio de los satélites de comunicación. A la dificultad de las intercepciones, estos servicios han respondido con la utilización de materiales cada vez más poderosos y desgraciadamente, cada vez más onerosos.

Las técnicas de análisis han adquirido una amplitud considerable a partir de la segunda guerra mundial y desde que sus instrumentos entraron en la era electrónica.

---

[32] *cfr.* Jean Pierre Alem, *El espionaje y el contraespionaje*, p.52

En el lenguaje del espionaje, las señales de inteligencia son conocidas como SIGINT (signal intelligence). Las intercepciones de ondas hertzianas constituyen la SIGINT. Prácticamente todas las agencias de inteligencia que recolectan información secreta usan el método SIGINT.

Las señales de inteligencia (SIGINT) son la única disciplina con un extenso e histórico pasado. La era moderna del SIGINT data desde la Segunda Guerra Mundial, cuando EE.UU. rompió el código militar japonés para invadir la isla Midway. Esta inteligencia le permitió a EE.UU. derrotar la flota superior de Japón. Se cree que el uso de SIGINT ha contribuido directamente a acortar la guerra por lo menos un año. Hoy, SIGINT continúa jugando un papel importante manteniendo el estado de superpotencia de los Estados Unidos.

SIGINT se subdivide en COMINT (Inteligencia de las Comunicaciones), que concierne a las transmisiones de mensajes en el sentido ordinario del término, mensajes expresados en el lenguaje escrito, cifrados o no, y el ELINT (inteligencia de señales electromagnéticas) que se ocupa de las emisiones no *significativas*: radar, telemetría, teleguía de instrumentos, ayudas para la navegación, etcétera.

En cuanto al ELINT, las indicaciones que permite recoger procuran, una vez tratadas mediante computadora, numerosas informaciones, a menudo interesantes y en ocasiones capitales: permiten descubrir la aproximación de aviones y misiles y desencadenar la alerta, identificar y localizar los materiales emisores, confundir las emisiones y así, por ejemplo, desviar, un misil –nuclear o no- de su blanco previsto, tal vez incluso devolverlo contra quien lo ha lanzado.[33]

El ELINT, desempeñara un papel esencial en un conflicto electrónico futuro; por ello se le han consagrado medios importantes en tiempos de paz. En Estados Unidos, la NSA (Agencia Nacional de Seguridad) está encargada de COMINT y

[33] *cfr.* Kurt D. Singer *Espionaje* p. 19

ELINT, en cooperación con la CIA y los servicios militares de información. Los conflictos locales de las últimas décadas han dado la posibilidad de experimentar sus materiales y métodos. Conocemos algunos de sus fracasos: los torpedos *Maddox* y *Turner Joy* bombardeados en 1964, en el mar de China; el Liberty, atacado en junio de 1967 por los buques de guerra israelitas (34 muertos); el *Pueblo*, capturado por la marina norcoreana en Wonsan, en enero de 1968.[34]

Todas estas actividades por su naturaleza secreta indican evidentemente que podemos conocer más los fracasos y no los éxitos, y es probable que estos sean más numerosos que aquéllos. Ningún gobierno va a comunicar a la comunidad internacional que gracias a sus actividades secretas han obtenido información confidencial o han cerrado un contrato multimillonario con alguna empresa extranjera.

Fuente: http://mediafilter.org/caq/echelon/CAQSecretPower.html

[34] Desde el punto de vista operativo, estas expediciones estaban dirigidas por la *Naval Intelligence*.

1.3.3 *Observación aérea*

Acabamos de referirnos a los dispositivos que permiten *oír más* y mejor. Se han creado simultáneamente otros dispositivos, para ver más y mejor, y, a la vez, para fijar las imágenes obtenidas. El problema que en este dominio se planteaba era alcanzar objetivos situados fuera del alcance de sus agentes; para hablar claro, los norteamericanos querían conocer las bases soviéticas en Siberia, y no tenían un "espía que saliese al frió"; la idea simple que se les ocurrió fue enviar aviones por encima de esos objetivos y fotografiarlos; la dificultad estaba en que los aviones tendrían que volar muy alto para no ser interceptados, y las fotos tendrían que fijar detalles los bastante pequeños para que fueran explotables. Los progresos paralelos de las técnicas aeronáuticas y fotográficas debían aportar la solución de ese doble problema y, en los años cincuenta, los norteamericanos pusieron en servicio el **U-2**, un avión cuyo rango de vuelo era de 16 000 metros, cuyas cámaras permitían identificar una rampa de lanzamiento de cohetes. Hacía tiempo ya que la primera bomba atómica soviética había explotado en septiembre de 1949.[35]

Avión espía U-2

Fuente: http://www.area51central.com/images/U2.gif

[35] *cfr.* Jean Pierre Alem, *El espionaje y el contraespionaje,* p.54

Los U-2 proporcionaron a los servicios norteamericanos "informaciones de un carácter vital".[36] El 1 de mayo de 1960, los soviéticos abatieron el aparato piloteado por Francis Gary Powers. Menos de dos años más tarde, los cubanos destruían el avión de R. Anderson. La explotación política de estos incidentes trajo por consecuencia el abandono del U-2. Los norteamericanos fabricaron aviones más perfeccionados, y luego aparatos sin piloto (Ryan 147, Ryan BGM34). El paso a la fase operativa de los satélites puso fin a esta generación de aparatos.[37]

1.3.4 *Los satélites*

El 4 de octubre de 1957 los soviéticos lograron la hazaña, considerada sensacional en su momento, de enviar al espacio un satélite artificial de la Tierra, el **Sputnik**.[38]El Sputnik permaneció en órbita durante 92 días y se desintegró en la atmósfera el 4 de enero de 1958. Llevó a cabo las primeras medidas de la densidad de la atmósfera y las primeras investigaciones de las transmisiones de ondas electromagnéticas a través de la Ionosfera.[39]

El suceso alcanzó una inmediata repercusión mundial e impactó fuertemente en medios políticos, científicos y militares de EE.UU. acelerando los planes para emularlo. La URSS, donde paradójicamente la trascendencia de la proeza es inicialmente subestimada, lanzará casi un mes más tarde un segundo satélite, de mayor tamaño y complejidad, pero esta vez con una perra llamada *Laika* a bordo para el estudio de los efectos de la ingravidez espacial.

---

[36] Allan Dulles, director de la CIA, en *La técnica de la información*.
[37] *cfr.* Jean Pierre Alem, *El espionaje y el contraespionaje*, p.54
[38] El *Sputnik* era una esfera de aluminio de 58 cm. de diámetro y pesaba 83 Kg. Tardaba 96.2 minutos en dar la vuelta a la Tierra.
[39] *cfr.* http://es.geocities.com/jose958/historia_satelites.htm -->

Desde esa fecha hasta fines de 1978, se han lanzado más de 2 mil satélites,[40] de la URSS y de Estados Unidos, pero también de China, Francia y las organizaciones espaciales europeas.

Satélite *Sputnik*

Fuente: http://142.26.194.131/aerodynamics1/Appendix/Aircraft/Graphics/u2_1.JPG

Apresurándose en la carrera por el espacio, los norteamericanos hicieron esfuerzos considerables para recuperar su retraso y, desde el mes de enero de 1958, pusieron en órbita el Explorer 1.[41]

El Explorer 1 pesaba 3kg. Este pequeño satélite logra en su viaje al espacio detectar el cinturón de radiación magnética que rodea a la Tierra, posteriormente este cinturón recibiría el nombre de su principal investigador James Van Allen.

[40] Fines de 1977: 704 lanzamientos de EEUU; 1077 de la URSS.
[41] *cfr.* http://www.cosmopediaonline.com/sputnik.html -->

Todos esos satélites aportaron importantes conocimientos al mundo científico, pues al ser equipados cada vez con mejores y más sofisticados instrumentos de medición, permitieron conocer las condiciones del espacio que rodea a la Tierra y, con ello, promover nuevos experimentos.

Los satélites están consagrados, en una proporción importante, a misiones militares; 78% para la extinta URSS, 38% en el caso de EEUU. En el dominio militar, las actuaciones de norteamericanos y ex soviéticos son generalmente paralelas y simultáneas. Este principio se corrobora en el caso que nos ocupa.[42]

Las misiones militares de los satélites son de cinco tipos: observación, telecomunicaciones, navegación, reconocimiento electromagnético, detección de misiles balísticos y de explosiones nucleares La misión de observación es particularmente interesante porque, jurídicamente, un satélite que pasa por encima de un Estado no viola su espacio aéreo; la observación puede por lo tanto extenderse a todas las regiones del planeta sin que se haya de meter incidentes diplomáticos. [43]

El aspecto fotografía fue uno de los que más ha avanzado, se han utilizado para fines climáticos hasta militares. Técnicamente, las fotografías se toman por medios clásicos o bien mediante la utilización de infrarrojo (fotos nocturnas) o de ondas de radar centimétricas (fotos de día o de noche en cualquier época). Actualmente es tal el poder de los satélites que son capaces de fotografiar desde el espacio la hora de un reloj. Es indudable que los satélites no sólo son utilizados para cuestiones de telecomunicaciones, su potencial les permite explotar otros ámbitos.

La observación puede responder a necesidades estratégicas o tácticas. En el primer caso, el poder de resolución –es decir, el diámetro mínimo de los

---

[42] *idem*
[43] *cfr.* http://es.geocities.com/jose958/historia_satelites.htm -->

objetos que puede descubrir la fotografía- debe ser entre 3 y 5 m, en el segundo es necesaria una alta resolución del orden de 0.5 m.

"La observación fue una de las primeras misiones militares confiadas a los satélites; la extinta URSS empleó para ese fin, desde 1962, los *Cosmos* y Estados Unidos, desde 1961, los *Samos*, y luego los *Discoverer*, los *Midas*, etc. Estos satélites de mediana resolución tienen órbitas circulares que pasan por los polos. Las fotografías se revelan a bordo y se transmiten a tierra por radio. Los satélites americanos que se encuentran fuera de la zona de visión radio de sus bases están vinculados por un satélite geoestacionario del Pacífico, el SDRS. La duración de vida de estos aparatos es de varios años."[44]

Cuando el estudio de las fotografías estratégicas hace aparecer la necesidad de un análisis más fino de ciertos puntos, se envía un satélite de observación táctica sobre los objetivos a precisar. Estos aparatos tienen órbitas elípticas, de bajo perigeo por encima de su objetivo (180 Km.). Se conoce un satélite de este tipo, el *Big Bird*, que no pesa menos de 12.5 toneladas.

Además de la extinta Unión Soviética y Estados Unidos, una tercera potencia está dotada hoy día de satélites de observación fotográfica: la República Popular de China lanzó tres en 1975 a partir de una base en Kan Su, pero éstos no han tenido más que una vida efímera, menos de sesenta días. Pero ciertamente los chinos han hecho progresos importantes a partir de esa primera experiencia.

"Los satélites de reconocimiento electromagnético tienen por misión *escuchar* todas las emisiones electromagnéticas y, más especialmente, escuchas por radar. En efecto, para facilitar la penetración en territorio enemigo de misiles balísticos portadores de ojivas nucleares, es indispensable conocer el dispositivo

---

[44] Jean Pierre Alem, *El espionaje y el contraespionaje*. Traduc. David Huerta, p. 57

de defensa del adversario que funciona a base de radar, y la frecuencia, modulación, velocidad de barrido e implantación de esos radares. Para obtener esas informaciones los norteamericanos pusieron en órbita, a partir de 1962, los satélites *Ferret*. La escucha por radar puede además utilizarse para la localización de submarinos. Probablemente es una misión de ese tipo la que cumplía un *Cosmos 954* soviético, portador de un rector nuclear, cuando se desintegró sobre Canadá en el mes de enero de 1978."[45]

Los satélites de detección de lanzamientos de misiles balísticos tienen un interés defensivo evidente, que es proporcionar un "tiempo de advertencia" lo mayor posible.[46] Los aparatos norteamericanos de ese tipo, los IMEWS, están situados en número de 6 u 8 en órbita casi geoestacionaria. Su equipo permite igualmente la detección de explosiones atómicas.[47]

Cada vez que aparece un arma nueva, los militares empiezan a estudiar la manera de neutralizarla o destruirla. Así ha sido ciertamente en el caso presente, y el satélite ha resultado un arma vulnerable; se ha intentado en primer lugar atacar las informaciones recogidas y generalmente trasmitidas por radio; el bloqueo de esa unión radial anula el interés del aparato; se ha tenido en cuenta en segundo lugar que el funcionamiento operativo de un satélite depende muy a menudo de estaciones terrestres (telecomandos). La perturbación de la unión tiene por tanto un efecto de neutralización.

Finalmente, se ha pensado en la destrucción del aparato mismo, acción grave, que constituye un *casus belli,*[48] pero que sin embargo se podría emprender en el curso de una guerra. La extinta Unión Soviética ha efectuado

---

[45] *Idem*
[46] La misión de detección de misiles balísticos, así como de los aviones que vuelan a baja altura y los blindados, corresponde a los *radares volantes* (Boeing 707 Awacs de los norteamericanos y de la OTAN, sistema MOSS de los soviéticos).
[47] *cfr.* http://www.hq.nasa.gov/office/pao/History/sputnik/sputorig.htm
[48] Una acción por un Estado contrataría a los intereses de otro y considerada como causa de guerra.

experimentos de destrucción de sus propios satélites, y los norteamericanos probablemente han hecho lo mismo.

Los primeros aparatos de destrucciones podrían ser los misiles antimisiles balísticos; pero el inconveniente de esas armas es que no son operativas, actualmente, a más de 1000 kilómetros. Otra opción de destrucción de satélites (ya que los misiles balísticos pierden control) es el láser, no para destruir otros satelices o para derribar alguna aeronave (el rayo de la muerte todavía pertenece a la ciencia ficción) sino para perturbar su propio equilibrio térmico y deteriorar algunos de sus componentes, para así lograr la autodestrucción.

Pero el arma más eficaz contra el satélite es otro satélite. Por ello ha aparecido, tanto en la extinta URSS como en Estados Unidos, una nueva generación de aparatos, los *cazadores* o *matadores*. Los experimentos de cita en el espacio de cambio de órbita prueban que se ésta persiguiendo activamente la puesta en práctica de esos nuevos materiales. La ventaja de los *cazadores* sobre los misiles es que no hacen funcionar más que cargas explosivas clásicas, en vez de cargas nucleares.

Aunque todavía es más difícil de realizar, se ha considerado incluso la captura de un satélite enemigo. Claro que primero se tiene que comprobar que el satélite se esta utilizando con fines de espionaje o militares, que en realidad es lo primero que se piensa ya que la mayoría de los satélites no oficiales o no detectados son utilizados para estos fines.

La aparición de los *cazadores* tuvo por consecuencia la puesta en funcionamiento de sistemas defensivos destinados a equipar los satélites amenazados: los sistemas pasivos, que consisten en suprimir los aparatos particularmente vulnerables; pero también sistemas activos: los satélites estarían provistos de dispositivos de detección de la aproximación, que orientarían y

desencadenarían las armas de a bordo. No es imposible que asistamos un día a verdaderas batallas entre los robots más perfeccionados que el hombre ha concebido hasta ahora.

1.3.5 *La información submarina*

Ocurren cada vez más cosas bajo el mar. Allí se produce la ronda perpetua de los submarinos nucleares. Allí se hunden a veces las *cápsulas de retorno*, portadoras de las informaciones recogidas por los satélites o las cajas negras de las aeronaves. Así pues las ventajas que ofrece el océano son aprovechadas por el espionaje. Es por tanto lógico que los países que tienen preocupaciones estratégicas a escala mundial hayan extendido sus investigaciones a esta parte del mundo submarino.

Este nuevo dominio de la información tiene dos aspectos: el primero se refiere a los sistemas que permiten escuchar bajo el agua y descubrir así el paso de los submarinos, los naufragios, las caídas de aviones o aparatos. Estas escuchas se fundan generalmente en la acústica submarina (sonar) y al parecer también, desde hace poco, en procedimientos magnéticos de detección, el láser y la detección de estelas térmicas. Todo ello es tarea de aviones, helicópteros, construcciones en la superficie, submarinos, y de *hidrófonos* de gran tamaño fijados en boyas sumergidas a diversas profundidades. Los norteamericanos han equipado con esos aparatos una red que "cubre" todos los océanos, el "Sea Spider"[49], que maneja la US Navy. Los soviéticos, por supuesto, crearon una red análoga y es probable que sus hidrófonos hayan registrado los ensayos del misil Tridente, lanzado por submarino.[50]

---

[49] Araña de mar.
[50] *cfr* Jean Pierre Alem, *El espionaje y el contraespionaje*. Traduc. David Huerta p. 61

El segundo aspecto, o mejor la segunda modalidad del submarino, consiste en explorar y si es posible recuperar los despojos que puedan constituir fuentes de información.

"Este procedimiento no es nuevo. Durante la guerra 1914-1918, el jefe naval británico, el almirante Reginald Hall envió un hombre rana a visitar los despojos de un submarino alemán que se hundió cerca de las costas inglesas, el UC-44, el recuperó así el código del navío. Ese mismo hombre rana penetró después en decenas de cascos de submarinos y recogió en esas expediciones los planos de los campos de minas alemanes y varios códigos. Gracias en parte a esos trabajos, el *Buró 400B* pudo descifrar los telegramas estratégicos y diplomáticos alemanes. Probablemente mediante una operación análoga los propios ingleses lograron en el curso de la Segunda Guerra Mundial, procurarse una máquina *Enigma,*[51] de la que obtuvieron el enorme beneficio ya conocido."[52]

Pero esas antiguas operaciones, realizadas con medios modestos, no permitían más que exploraciones breves y poco profundas. Todo cambia con los métodos modernos que son, como veremos, gigantescos, y que permiten recoger despojos a gran profundidad. En 1972, los norteamericanos se procuraron así el equipo electrónico de un navío, después de su naufragio en el mar de Japón, y una bomba atómica dejada caer por un avión. El mismo año, en colaboración con los ingleses, habrían recuperado en el mar del Norte el aparejo electrónico de un avión soviético. Una operación de muy diferente envergadura, la "*Operación Jennifer*", tuvo lugar en 1974.[53]

"En 1968, un submarino soviético de la clase G, armado de torpedos nucleares, se hundió al noroeste de las islas Hawai. La explosión que provocó el

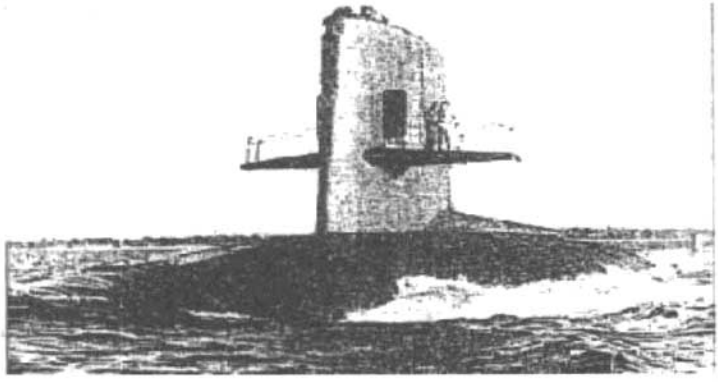
---

[51] Enigma, una maquina *electro-mecánica* con una serie de tambores y ruedas, utilizada por los alemanes para encriptar sus mensajes de radio.
[52] *Ibidem* p.60
[53] *cfr.* Jean Pierre Alem, *El espionaje y el contraespionaje,* p.62

naufragio fue registrada por uno de los hidrófonos de la red Sea Spider, de manera que un buque especializado de la marina norteamericana, el *Mizar*, logró fotografiar el submarino a 5 mil metros de profundidad."[54]

"Sacar del mar un despojo de más de 3 mil toneladas, hundido a semejante profundidad, era una empresa jamás realizada y que parecía irrealizable. El gobierno norteamericano decidió sin embargo intentarlo. La operación se le confió a la CIA, y se le atribuyó al efecto un presupuesto aproximado de 350 millones de dólares.La CIA actuó bajo una cobertura proporcionada por el multimillonario Howard Hughes, que fundó con ese objeto una sociedad de explotación de nódulos polimetálicos, además hizo construir dos buques especiales: un navío de 36 000 t. de desplazamiento, el *Glomar Explorer*, y una panga sumergible "del tamaño de un campo de fútbol". La operación tuvo lugar en julio y agosto de 1974. Rodeada de un riguroso secreto, fue revelada en el mes de marzo de 1975. Según la CIA, el éxito fue parcial: sólo se logró recuperar una tercera parte del casco. Pero es posible que la agencia norteamericana haya juzgado oportuno disimular la amplitud de su éxito."[55]

Submarino espía *Scorpion (1960)*



Fuente: http://members.aol.com/bear317d/scorpion.htm

[54] Jean Pierre Alem, *El espionaje y el contraespionaje* p. 63
[55] *Idem*

1.4 Espionaje espacial

> *"Durante la segunda mitad del siglo XX, las máquinas y las computadoras empezaron a ejecutar los trabajos que con anterioridad hacían los hombres. La tecnología de los chips de silicio, según se afirmó, era más confiable, más eficiente, más capaz. La industria del espionaje no fue la excepción. Sin embargo, en ocasiones, los espías humanos encuentran maneras de devolver el golpe..."*[56]

Posiblemente cuando se lanzo el primer satélite artificial al espacio (el Sputnik), pocos imaginaron las posibilidades que brindaría la tecnología satelital en cuando a la forma de comunicarnos o para ofrecer un reporte meteorológico más exacto, pero seguramente nadie imagino la manera en que los satélites estarían involucrados de manera tan directa con la cuestión del espionaje, convirtiéndose en la actualidad en una herramienta indispensable para llevar a cabo espionaje internacional.

"Les Brown apenas podía creer a sus ojos borrosos, allí, en su puerta, estaban un policía y un piloto de helicóptero de la RAF[57] con un traje de vuelo: su expresión era de desagrado y sorpresa a las 6:00 horas, mas el motivo que tenían para sacar a Les de su cama era todavía más sorprendente. Helicópteros y barcos habían pasado la noche en el intento de localizar la fuente de una misteriosa señal de auxilio. Los operadores de radar en Toulouse, Francia, fijaban ese sonido en la región Firth of Clyde, en Escocia; el personal del centro de investigación Pitreavie, de la estación de rescate Fife y de la base del submarino nuclear Faslane, habían localizado el sitio exacto en la humilde casa de Les, en Erskine, cerca de Glasgow. El culpable era un radiofaro defectuoso guardado en la parte superior del armario, en la habitación desocupada de Les. El aparato,

---

[56] Roger Boar, *Los espías y maestros del espionaje más grandes del mundo*. Traduc. Luz Broissin, p. 249
[57] R.A.F. Siglas de la *Royal Air Force*, Real Fuerza Aérea, del Ejercito Inglés.

fue comprado en 10 libras y fue destinado al bote de pesca en el que trabaja Les. Se había desencadenado una cacería que costó cerca de 20 000 libras."[58]

Los periódicos se divirtieron con esta historia, transcurrida el 16 de julio 1983. Sin embargo, tuvo un significado mucho más allá de la simple diversión. La primera noticia sobre la señal de auxilio llegó de un satélite espacial ruso, y su capacidad para captar un blanco tan pequeño desde kilómetros de distancia en órbita era prueba devastadora de la efectividad atemorizante de la vigilancia espía en el cielo.

"En seis semanas, un efecto mucho más serio demostró que también Occidente tiene ojos electrónicos entrenados en todas partes del globo. Cuando los caza-bombarderos rusos Mig derribaron el vuelo 007 de Korean Airlines y a sus 269 pasajeros inocentes en el cielo nocturno sobre la isla Sakhalin, entre la tierra firme soviética y Japón, un trabajador del servicio de inteligencia norteamericano asentó: *"Es casi seguro que supimos antes que Moscú lo que los pilotos de los Mig hacían y decían"*. Era un argumento invaluable en una crisis internacional que consternó al mundo. Además, explicó con exactitud por qué la tecnología de la era espacial es ahora responsable del 85% de la recopilación de datos en el espionaje moderno."[59]

Los espías más valiosos ya no son agentes humanos[60] de la CIA o de la extinta KGB sino son ahora satélites sofisticados, barcos espías, estaciones ultra sensitivas para escuchar en tierra y bancos complejos de computadoras que trabajan las 24 horas del día.

"Los vigilantes de seguridad más importantes de Occidente son: la Agencia de Seguridad Nacional Norteamericana (NSA), con base en Fort

---

[58] Roger Boar, *Los espías y maestros del espionaje más grandes del mundo*. Traduc. Luz Broissin, p. 249.
[59] *Ibidem* pp. 250-251
[60] Aunque no debemos de olvidar que el factor humano es el principal motor del espionaje, los aparatos son una consecuencia.

Meade, un terreno de 4.45 hectáreas en frondosa tierra de cultivo en Maryland, 48 kilómetros al norte de Washington, y el Centro de Comunicaciones del Gobierno Británico, en Cheltenham, Gloucestershire (CCGB)). Ambos centros emplean alrededor de 140 000 personas y su funcionamiento tiene un costo estimado de 15 billones de dólares al año. De acuerdo con un ex empleado de la NSA, pueden "mantener una configuración, momento a momento, de casi todo lo que sucede en el mundo que sea de importancia militar o política". Un hombre que trabajó en el CCGB declaró: "Pueden localizar cualquier cosa que se mueva, desde una taza de té hasta una bomba atómica". Esa habilidad se obtiene al observar el mundo desde todos los ángulos."[61]

Los espías han estado en el cielo desde el siglo XIX, cuando generales enviaron globos de aire caliente sobre las líneas enemigas para valorar su fuerza y táctica. Durante la Segunda Guerra Mundial, las cámaras añadieron una nueva dimensión a los ojos que todo lo ven (de los pilotos de los aviones) y culminaron en la década de los cincuenta con vuelos a gran altitud e los jet U2 sobre Rusia, por los pilotos norteamericanos. "Sin embrago, el 5 de mayo de 1960, el piloto de un U2, Francis Gary Powers, fue derribado sobre Sverdlovsk y se levantó una llamarada de publicidad embarazosa. Meses antes, otro avión U2 fue forzado a aterrizar. Nunca se volvió a saber de su tripulación de ocho hombres. El presidente Eisenhower prohibió más vuelos y en 1963, poco después que Powers fue puesto en libertad a cambio del espía soviético Rudolf Abel, el primer satélite sin tripulación quedó en órbita."[62] En dos años, los vigilantes del espacio demostraron su valor, pues detectaron la producción de plutonio en una fábrica en el interior de Mongolia a la que ningún agente occidental podía llegar y alertaron a los Estados Unidos sobre la primera bomba nuclear probada en China. Desde entonces, los satélites han sido perfeccionados hasta convertir su potencial de espionaje en algo sorprendente, como lo demostraron con la detección de la señal de auxilio en Erkine y la tormenta sobre el vuelo 007.

---

[61] *Idem*
[62] Vernon Hinchley, ***Espionaje al desnudo***. Traduc. T.3 de Tovar, p. 46

Fuente: http://mediafilter.org/caq/echelon/CAQSecretPower.html

Las cámaras a 321 kilómetros de altura pueden enfocar objetos de no más de 30.4 centímetros de longitud. Las cámaras que se encuentran a bordo de los satélites norteamericanos *Big Bird* pueden enfocar los números de las placas de un automóvil y los encabezados de los periódicos con sus lentes de 243.8 centímetros. Detectores infrarrojos señalan la ubicación de misiles subterráneos, al medir los cambios en la temperatura de la tierra. Censores de sonido interceptan las comunicaciones por radio, teléfono y microondas. Las orbitadores norteamericanos han captado conversaciones radiotelefónicas entre los miembros del Politburó que se dirigen a reuniones en el Kremlin en limusinas separadas. Otros satélites están programados para localizar partes de cohetes, desperdicios nucleares y submarinos. Incluso algunos pueden enviar señales falsas a los técnicos soviéticos que prueban misiles.[63]

El espionaje aéreo es apoyado por la piratería de secretos sobre y bajo los mares. Moscú dirige en forma magistral los movimientos de cientos de barco de pesca y barcos mercantes. Llegan a puertos occidentales para recoger información. Recorren las costas importantes y localizan a barcos de guerra de la OTAN en entrenamiento. A principios de 1982, algunos de éstos siguieron a la

[63] *cfr.* http://www.hq.nasa.gov/office/pao/History/sputnik/sputorig.htm

fuerza operativa británica hacia el Atlántico Sur, para la recuperación de las Islas Malvinas. Un año más tarde, un barco mercante ancló a kilómetro y medio de Florida para observar cómo los científicos de los Estados Unidos probaban un misil Trident. Un observador norteamericano comentó que tenía "tantos misiles electrónicos y antenas parabólicas que corría el peligro de naufragar".[64]

La flota norteamericana también incluye barcos espías, los cuales anclan cerca de los sitios donde hay conflicto para escuchar el tráfico de radio y teléfono. "Uno de éstos fue atacado por jets de Israel en el Mediterráneo durante la Guerra de los Seis Días, en 1967. Un año después, se presentó un desastre todavía mayor. Cuatro cañoneros de Corea del Norte capturaron al barco *Pueblo* de los Estados Unidos en aguas internacionales, el 23 de enero de 1968. La tripulación de 82 hombres, ocupada en inspeccionar las instalaciones de barcos y radar a lo largo de la costa, fue mantenida prisionera durante 11 meses, en lo que un desertor checo describió más tarde como una cuidadosa conspiración del Kremlin planeada para humillar a los Estados Unidos, desanimar el espionaje norteamericano y demostrar a los líderes de Corea del Norte que Rusia podía ser un aliado mucho más poderoso que China. El complot tuvo éxito mucho más allá de los sueños atrevidos de Moscú. Además el golpe de propaganda, los comunistas obtuvieron detalles de las operaciones norteamericanas en el Pacífico, así como de las claves que permitieron a la extinta KGB descifrar miles de mensajes que antes eran inescrutables y que estaban guardados en cintas".[65] Una investigación de los Estados Unidos recomendó acción disciplinaria contra el comandante Lloyd Mark Bucher y su principal oficial de inteligencia, pero el secretario de Marina John H, Chafee dijo *"Ya han sufrido suficiente"*.[66]

El espionaje en el mar también llega por debajo de las olas. Suecia y Noruega dejaron caer cargas de profundidad sobre submarinos soviéticos

---

[64] Vernon Hinchley, *Espionaje al desnudo*. Traduc. T.3 de Tovar, p. 253
[65] *Ibidem* p.254
[66] *Idem*

sospechosos en las aguas profundas a lo largo de sus costas a principios de la década de los ochenta. En junio de 1983, un equipo sofisticado de monitoreo acústico fue descubierto en el lecho oceánico cerca de la costa occidental de los Estados Unidos. Era un aparato ruso para seguir los movimientos de los submarinos nucleares de los Estados Unidos; sin embargo, nadie supo cómo había sido instalado y desde cuándo estaba allí.

También en tierra la vigilancia electrónica ha sido refinada hasta alcanzar niveles sorprendentes. NSA y el CCGB tienen una red de 2000 estaciones de escucha ultra sensibles alrededor del mundo, desde Alaska hasta Australia, desde Belice hasta Botswana y desde Canadá a Chipre. Hay incluso dos en el norte de China, cuya operación es permitida por los chinos a cambio de compartir información sobre los movimientos de las tropas soviéticas. Durante el derribamiento del vuelo 007 en agosto de 1983, esas estaciones, además de otras en Taiwán, Hong Kong, Japón y Corea del Sur, escuchaban junto con los satélites los comentarios concisos de los pilotos de los Mig y de sus controladores en tierra.

Información de todos estos ojos y oídos llega a los centros de recopilación y análisis a una velocidad de más de un millón de palabras por segundo. En Fort Meade y en Cheltenham, los bancos de computación codifican, traducen, cotejan, y analizan al instante los mensajes interceptados. Cerebros electrónicos capaces de registrar cuatro millones de caracteres por segundo, y de leer y clasificar cualquier periódico en el tiempo que toma pronunciar su título, son programados para detectar las palabras clave y sonar la alerta cuando sucede algo fuera de lo común. Sólo Fort Meade examina 40 toneladas de documentos al día, con clasificaciones detalladas de información mundial diplomática, política, militar y económica para la Casa Blanca y los espías maestros en Washington.

Los observadores occidentales aseguraban saber al instante si era lanzado un misil del Pacto de Varsovia, cuando un avión se elevaba y cuando se movilizaba un ejército. Podían reconocer a todos los pilotos del bloque soviético por su señal de llamada. NSA y CCGB supieron con anticipación, en aparte a través del tráfico de radio aumentando, sobre la crisis cubana de misiles en 1962 y la invasión soviética de Checoslovaquia en 1968. Las bases de escucha británicas ayudaron a los Estados Unidos a captar las intenciones del enemigo durante la guerra de Vietnam, y los Estados Unidos devolvieron el favor al pasar los mensajes argentinos durante el enfrentamiento de las Islas Malvinas. Cuando la Gran Bretaña negoció la entrada al Mercado Común, el conocimiento sobre las actitudes de otros gobiernos europeos fue más que útil en la negociación.[67]

De esta manera apreciamos como los gobiernos utilizan sus tecnologías de una manera más seductora, presumen sus logros, presumen su tecnología, presumen sus éxitos, se mofan de los fracasos del enemigo. Y siempre cuidando sus intereses. Parece como una especie de juego que consiste en quien espía más y mejor.

[67] *cfr.* Claude Guillaumin, ***Los grandes enigmas del espionaje***. p. 52

CAPÍTULO 2

EL SISTEMA INTERNACIONAL DE ESPIONAJE: CASO ECHELON

2. El sistema internacional de espionaje: caso ECHELON

En los últimos años los conceptos de seguridad y defensa han venido convergiendo en múltiples facetas, tratando de atender los intereses globales de los Estados de forma eficiente. Día a día emergen amenazas que atentan la seguridad nacional de un país y que ponen en alerta a la comunidad internacional, para afrontar tal situación los gobiernos llegan a implementar acciones poco conocidas.

Quienes han navegado por internet consultando páginas de noticias europeas seguramente han leído de algo llamado Echelon[68], que al parecer es una especie de red de espionaje internacional capaz de interceptar comunicaciones a nivel mundial y la cual esta liderada principalmente por los Estados Unidos, este último consistentemente lo ha negado. Pero en el año de 1999 Australia (uno de los participantes del proyecto) admitió débilmente que algo había de cierto y a fines de febrero del 2000 se produjo un escándalo, cuando el Parlamento Europeo denunció que Echelon analizaba todo el tráfico de internet, así como conversaciones telefónicas y de fax de todo el mundo.

Paginas noticiosas, investigadores, aficionados señalan que Echelon es la red mundial de espionaje, que todo lo ve, que todo lo escucha y que todo lo lee. Con los recursos financieros y tecnológicos colosales con los que cuenta esta red y con los gobiernos que están detrás de ella, no suena tan descabellada esta idea.

[68] Escala de cuerdas, en inglés, también significa escalón.

2.1 Historia de Echelon

Al concluir la Segunda Guerra Mundial, EEUU y el Reino Unido firmaron un tratado altamente secreto conocido como acuerdo *UKUSA* (***U***nited ***K***ingdom-***U***nited ***S***tates of ***A***merica[69]). A este acuerdo, rubricado en 1948 y oculto hasta 1999, se unieron Canadá, Australia y Nueva Zelanda como países "terceros".

Bajo el acuerdo UKUSA, los países de habla inglesa acordaron dividirse la vigilancia del mundo. En un principio Gran Bretaña y Estados Unidos vigilarían toda Europa, África y la extinta URSS. Canadá cubriría latitudes del norte del mundo y las regiones polares. Y Australia cubriría Oceanía.

Los acuerdos fijaron los mismos procedimientos, los mismos objetivos, los mismos equipos y los mismos métodos que las agencias de *Sigint* usarían. Otros países como Noruega, Dinamarca, Alemania y Turquía firmaron los acuerdos de *Sigint* con los Estados Unidos y Gran Bretaña.

Los Estados Unidos y el Reino Unido ya contaban con una larga trayectoria de cooperación en materia militar y de espionaje que durante la Segunda Guerra Mundial se afianzó hasta el punto de compartir ambos países los éxitos criptográficos logrados al desenmascarar, entre otras, la clave de los nazis en la máquina *"Enigma"* o la japonesa *"Púrpura"*[70]. Con la firma de aquel pacto de posguerra lo único que hicieron EEUU y el Reino Unido fue perpetuar su acuerdo total de colaboración ante la nueva era que se iniciaba: la Guerra Fría.

---

[69] Reino Unido – Estados Unidos de América.
[70] *cfr* http://www.rebelion.org/cibercensura/echelon071102.htm

Durante los años 50 y 60, los países firmantes del pacto UKUSA aprovecharon el potencial militar de espionaje de señales puesto en marcha antes de la Segunda Guerra Mundial y lo siguieron explotando para vigilar al enemigo soviético y sus aliados del Pacto de Varsovia. Grandes antenas de alta frecuencia para escuchar comunicaciones por radio, junto a diversos artilugios tecnológicos para interceptar los cables submarinos, sirvieron a estas naciones para escuchar a la URSS, así como para vigilar el potencial armamentístico nuclear soviético y de sus países satélites.

En un principio el pacto UKUSA, estaba dedicado a interceptar la información de los países del Pacto de Varsovia, pero después del fin de la Guerra Fría sus actividades de espionaje se expandieron hacia otras áreas, como el espionaje industrial y de empresas.

Las comunicaciones avanzaron y en la década de los setenta se lanzaron los primeros satélites comerciales destinados a las comunicaciones civiles. Fue entonces cuando nació la llamada red espía "Echelon".

Para ese entonces varias naciones habían coordinado sus esfuerzos para lanzar los primeros satélites Intelsat, a los que seguirían otras redes como Inmarsat, Eutelsat, Arabsat, etcétera. Diversos autores que han investigado este caso durante los últimos años ya han demostrado que, cada vez que INTELSAT lanzaba un nuevo satélite, los países del tratado UKUSA respondían instalando una nueva antena parabólica gigante en una de sus bases de espionaje para interceptar sus emisiones.[71]

El sistema "Echelon" se equipó con ordenadores a los que se dotó de un programa denominado "Diccionario", que sirve para seleccionar los mensajes interceptados en función de diversas palabras clave, algo bastante similar al

[71] *cfr* http://www.rebelion.org/cibercensura/echelon071102.htm

funcionamiento de los buscadores de internet. Para los países del tratado UKUSA era necesario poner en marcha un sistema automatizado que agilizara el trabajo a sus empleados y aminorase los costos del programa de espionaje global. Hasta ese momento, criptólogos[72] militares, traductores y analistas trabajaban en decenas de bases por toda la Tierra para interceptar, criptoanalizar, traducir y producir informes de inteligencia para las autoridades de los países anglosajones. Pero la burocracia, junto al aumento de las comunicaciones, hacía imposible mantener un sistema manual por más tiempo y se decidió implantar uno automatizado que desbrozara la ingente cantidad de mensajes interceptados y seleccionara sólo aquellos que pudieran ser interesantes para los analistas[73].

Las cinco agencias de inteligencia que constituyen el pacto UKUSA son:

De Estados Unidos de América: *National Security Agency*, NSA (Agencia Nacional de Seguridad), creada en 1952. Del Reino Unido: *Government Communications Headquarters, GCHQ* (Cuartel General de Comunicaciones), creada en 1952. De Nueva Zelanda: *Government Communications Security Bureau, GCSB* (Agencia de Seguridad de Comunicaciones del Gobierno), creada en 1977. De Canadá: *Communications Security Establishmen, CSE* (Establecimiento de Seguridad de las Comunicaciones), creada en 1946. Y de Australia: *Defence Signals Directorate, DSD* (Consejo de Administración de Señales de Defensa), creada en 1946.

Esta alianza creció de los esfuerzos cooperativos para interceptar transmisiones de radio durante la Segunda Guerra Mundial. La alianza se formalizó en un acuerdo escrito en 1948 y apuntó principalmente contra la URSS.

---

[72] Personas que se encargan de enmascarar y desenmascarar comunicaciones.
[73] *cfr* http://www.rebelion.org/cibercensura/echelon071102.htm

Estas agencias son hoy las más grandes organizaciones de inteligencia en sus respectivos países. Por décadas, antes de la introducción del sistema Echelon, los aliados de UKUSA hicieron operaciones de recopilación de inteligencia una para cada otra, pero después cada agencia procesaba y analizaba las intercepciones para sus propias estaciones.

La estación más importante del acuerdo UKUSA es Menwith Hill localizada en Inglaterra la cual fue establecida en 1956 por la US Army Security Agency (ASA)[74]. Es una base de acre celosamente custodiada que a simple vista cuenta con muchas antenas parabólicas y domos. Sus operaciones iniciales se enfocaron en monitorear cables internacionales y comunicaciones de microonda que atravesaban la Gran Bretaña.

A principios de los años sesentas Menwith Hill fue uno de los primeros lugares en el mundo en recibir las primeras computadoras sofisticadas de IBM, con las cuales la NSA automatizó todos sus procesos como el de escrutinio de listas.[75] Desde entonces, Menwith Hill ha "colado" mensajes internacionales, telegramas, llamadas telefónicas de ciudadanos, además de seleccionar información de corporaciones o gobiernos de índole político económico o militar que interesen a los Estados Unidos.

Con el avance de la tecnología también se fueron implantando mejoras en el programa "Echelon", que actualmente permite a los países del tratado UKUSA operar sus bases de espionaje vía satélite prácticamente por control remoto. Actualmente, analistas y técnicos dominan desde muy pocas bases un trabajo altamente automatizado que antes tenían que desarrollar centenares de especialistas en cada puesto de interceptación.

---

[74] Agencia de Seguridad del Ejercito.
[75] *Idem*

2.2 Echelon en nuestros días

Durante el año de 1998 cuando los medios de comunicación electrónicos empezaban a prestar atención a Echelon. Por aquel entonces, esta gigantesca red de espionaje electrónico, que traspasa fronteras y vulnera constituciones, apenas merecía el interés de unos pocos.

Había pocos datos concretos y era demasiado fácil calificar de paranoico a quien se atrevía a insinuar que un sistema de tal envergadura pudiera tener existencia real. Sobretodo partiendo de la base que el simple ciudadano podía ser objeto de vigilancia por parte de los gobiernos más poderosos del mundo, algo bastante extremo para el ciudadano que sólo ve su correo electrónico de vez en cuando.

El día 5 de septiembre de 2001, el Pleno del Parlamento Europeo aprobó una resolución histórica donde denunciaba la existencia de una red de espionaje de las comunicaciones operada por Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda. Su denuncia cayó en saco roto apenas seis días después. El 11 de septiembre de 2001, Al Qaeda atentó contra los Estados Unidos. Todos los países de la UE se unieron a la guerra contra el terrorismo promovida por George W. Bush y para luchar contra el terrorismo, "Echelon" es un arma esencial.

Muchos rumores han predominado durante los últimos años (de 1998 a la fecha), la mayoría provenientes de Europa que van desde ciudadanos hasta empresas transnacionales, estos rumores tomaron más fuerza con el aparecimiento de internet, se hablaba de un posible sistema internacional encargado de espiar o vigilar el mundo. Efectivamente el sistema existe y es conocida como Echelon.

Con recursos financieros colosales y con la tecnología más sofisticada (y a la vez desconocida) Echelon es la mayor red de espionaje y vigilancia internacional que el mundo jamás haya conocido. La red es operada a escala mundial por los Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda (acuerdo UKUSA).

La red permite interceptar y monitorear en todo el planeta millones de comunicaciones al día, transmitidas vía satélite como lo son llamadas telefónicas, videoconferencias, e-mails y faxes.[76] Para esto, utiliza 120 satélites, potentes computadoras, estaciones de vigilancia a lo largo del planeta, que reciben, analizan y ordenan la información capturada por los satélites de comunicaciones.

La ultra secreta *National Security Agency,* (Agencia Nacional de Seguridad) de 38 000 empleados y 4 000 millones de dólares de presupuesto es la agencia estadounidense que lidera el proyecto.[77] Recordemos a sus colegas:

- de Gran Bretaña, *Government Communications Head Quarters,* (Cuartel General de Comunicaciones).
- de Canadá, *Communications Security Establishment,* (Establecimiento de Seguridad de las Comunicaciones).
- de Australia, *Defense Signals Directorate,* (Consejo de Administración de Señales de Defensa).
- de Nueva Zelanda, Government Communications Security Boreau, (Agencia de Seguridad de Comunicaciones del Gobierno).

Se ha demostrado que los Estados Unidos, junto a sus países aliados, pueden interceptar todas las comunicaciones por satélite, buena parte de las

---

[76] *cfr* http://fly.hiwaay.net/~pspoole/echelon.html -->
[77] *cfr* www.nsa.gov

que se realizan por cables submarinos y una importante cantidad del tráfico de internet. Se insinúa también que son capaces de interceptar los cables submarinos de fibra óptica, aunque esto sólo es posible si se tiene acceso a los puntos donde salen a la superficie o en aquellos lugares en los que se instalan amplificadores para potenciar la señal antes de volver a introducirla en el cable para que siga su camino. Así pues, cualquier fax o llamada telefónica internacional, videoconferencia o correo electrónico que pase por un nodo de comunicaciones *"pinchado"*[78] por una de estas agencias de inteligencia de señales, es susceptible de ser interceptado.

Echelon es un sistema de interceptación, clasificación y evaluación de las telecomunicaciones, es un sistema tan real como poderoso, y tan eficaz como desconocido. Incluso los programas que brindan seguridad en internet no son suficientes o sólo son un disfraz que no impiden el espionaje *on line*.

Si fuese solamente eso, no se diferenciaría de otros esquemas similares puestos en marcha por los servicios de espionaje de todo el mundo, como algún satélite sospechoso que ande por ahí. Echelon no sólo es un programa de computadora en la computadora o algún aparato que graba tus conversaciones telefónicas. Echelon tiene algunas características que lo hacen único:

En primer lugar, es internacional tanto en ámbito como en composición. Echelon está formado por un *"club"* de diversas naciones, como se dijo anteriormente. Cada uno de estos países tiene un campo de actuación y comparte con los otros miembros del *club* sus descubrimientos. "Este proceder, además de asegurar una mayor cobertura, permite evadir espinosos problemas legales: puesto que la NSA norteamericana tiene prohibido por ley espiar dentro

[78] *pinchado* es hacer clic en el mouse de la computadora.

de los Estados Unidos, le basta con pedir la información a sus colegas del Reino Unido o de Canadá para obtenerla.

En segundo lugar, Echelon fue diseñado para que se comporte como una entidad inteligente. No se limita a interceptar mensajes y re-transmitirlos, ya que el enorme volumen de comunicaciones existente lo haría inviable. Por ello, se ha apelado a procedimientos informatizados de reconocimiento de voz y de contexto, y de búsqueda de palabras. Los mensajes intervenidos son cotejados en un "diccionario" en busca de concordancias. Si se halla un mensaje que incluya las palabras Bush y asesinato, el mensaje es enviado a donde corresponda. Es como una red de deriva inteligente, que solamente captura los peces que le interesa. Claro que los peces, ignorantes de la existencia de la red, siguen su camino creyéndose a salvo.

En tercer lugar, y a diferencia de otros muchos sistemas, Echelon fue diseñado específicamente para captar y procesar grandes cantidades de información en redes de transmisión CIVILES. Es decir, si Echelon está espiando comunicaciones comerciales y particulares no es porque se haya reconvertido tras el final de la guerra fría; simplemente, sigue haciendo el trabajo para el que ha sido diseñado. Las redes de telecomunicaciones militares ya tienen sus espías electrónicos. Echelon se ocupa de la mina de las comunicaciones civiles: telefonía fija, móvil, fax, internet... como dicen los norteamericanos *"usted lo nombra, yo lo tengo"*.[79]

Dados los ataques terroristas en aviones, trenes, embajadas, edificios públicos, y demás, esta aplicación no parece descabellada, si con esta escucha se logra salvar vidas inocentes y eventualmente, mantener la paz.

---

[79] *Idem*

Lo que en cambio es alarmante es que parecería que el análisis no se restringe a este tipo de espionaje civil, sino que también se habla directamente de espionaje comercial en favor de las multinacionales de los Estados Unidos y en perjuicio de sus competidoras europeas. De esta manera estaríamos en presencia de un sistema militar que escucha conversaciones civiles, pero que paradójicamente se estaría utilizando para fines comerciales.

El conflicto aparece cuando este control clandestino de las transmisiones se ejerce contra empresas que están en plenos acuerdos con un cliente, rivales de los grupos norteamericanos que Echelon busca privilegiar, cuando se trata sobre información acerca de patentes aún no registradas o sobre temas de propiedad intelectual, o cuando la vigilancia se extiende a las comunicaciones entre particulares. En internet, Echelon está catalogado como el arma de espía del gobierno estadounidense y por ello fue objeto de "represalias" por cientos de usuarios. En octubre se estableció un "*Jam Echelon Day*" ó "Día de obstrucción de Echelon". [80] Diversos grupos internacionales para la defensa de los derechos civiles y personas de todo el mundo comenzaron a bombardear el sistema a través de la red y de las líneas telefónicas con palabras como "terrorismo" con la esperanza de que el sistema entrará en crisis, pero sin lograr hasta ahora su objetivo. Súbitamente, Echelon ha dejado de ser un mito y ha pasado a ser tema de animado debate en respetabilísimos foros internacionales, además de convertirse en portada de diarios y revistas.

2.3 Funcionamiento de Echelon

El espionaje es un arte oscuro, y la verdad acerca de quien esta haciendo que, a quien y por que, no ha sido despejada (incluso para aquellos

[80] http://www.diarioti.com/noticias/1999/oct99/15192440.htm -->

involucrados). Con el funcionamiento de Echelon se intenta averiguar la esencia y la magnitud de un sistema que esta obstinado por la compleja naturaleza de la tecnología.

No obstante, sin el manual de operación, o el instructivo, es todavía posible construir un cuadro razonable que nos indique su funcionamiento. Sí es verdad o no, es imposible de determinar. Lo siguiente son conjeturas informadas de hechos pertinentes.

Echelon funciona con una amplia red de computadoras conectadas a siete estaciones principales alrededor del mundo que reciben, analizan y ordenan la información capturada por los satélites de comunicaciones.

El objetivo de Echelon es interceptar información secreta y pasarla a aquéllos que la necesitan saber. **Es decir, intercepta, clasifica y evalúa la información.**

La fuente principal de información de Echelon son las señales electrónicas SIGINT (Signal Intelligence). Digamos que aquí se obtiene la información "cruda". Esta información puede obtenerse de transmisiones de radio o de cables de fibra, con sus muy pocas excepciones. Las señales inalámbricas son las que mejor pueden ser interceptadas mientras que las trasmisiones de cable necesitan una intervención más "física".

La mayor frecuencia de interés es la frecuencia VHF[81] y las frecuencias más altas, aunque la onda corta ha sido tradicionalmente usada por el ejército y las agencias de inteligencia, pero sus características poco avanzadas la han llevado a ser poco utilizable.

---

[81] VHF, siglas de 'frecuencia muy alta' (en inglés, Very High Frequency), banda de frecuencias de radio comprendidas entre 30 y 300 megahercios (MHz). Esta frecuencia se utiliza para emisiones FM (frecuencia modulada) y de radioaficionados, así como para transmisiones de televisión.

La frecuencia VHF y sobre todo las señalas de radio viajan algunos cientos de millas para llegar a su destino. Estas transmisiones son detectables desde el espacio, y es aquí donde Echelon hace uso de una gran variedad de satélites de monitoreo. Pero éstos no son los nombres por los que ellos son actualmente conocidos. Estos satélites pueden escuchar directamente de teléfonos móviles (celulares) o de transmisiones de microondas que pueden estar conectadas a una base de estaciones y esta a su vez a una red central, o también escuchar las redes de microonda que muchos países todavía mantienen como parte de su infraestructura básica. [82]

Asimismo siempre ha sido normal que algunas señales vayan más allá de su destino y terminen por perderse en el espacio, donde los satélites de Echelon las están esperando. Se piensa que ésta es la fuente de mayor información de Echelon.

Una gran parte de Echelon esta dedicada a monitorear la Organización Internacional de Comunicaciones por Satélite (INTELSAT), esto gracias a las estaciones con las que cuentan todos los países del tratado UKUSA. Existen también estaciones auxiliares de Echelon cerca de las estaciones oficiales de INTELSAT cuyo objetivo es monitorear todas sus actividades relacionadas a transmisiones de datos.

Incluso INMARSAT (Organización Internacional de Comunicaciones Marítimas por Satélite) tiene vínculos con Echelon, con el gobierno estadounidense, con la NSA, con agencias de inteligencia y tiene su propio sistema de monitoreo.[83]

---

[82] *cfr* http://news.zdnet.co.uk/story/0,,s2079849,00.html -->
[83] *Idem*

Las señales recaudadas por los satélite no son analizadas por cada una de las estaciones del pacto UKUSA, en lugar de eso, estas señales son encriptadas[84] y difundidas por su estación correspondiente; ya que cada estación tiene la responsabilidad de cumplir con la vigilancia de una cierta región geográfica. Algunas de las estaciones tienen lugar no muy lejos de las embajadas que manejen información altamente importante para los integrantes del pacto UKUSA o cerca de redes locales de señales de microondas o simplemente donde existan *links*.[85] "Aquí es donde los servicios tecnológicos favorecen la labor, compañías como la Applied Signal Technology ofrece un aparato capaz de procesar simultáneamente 12,000 canales de información."[86]

Una vez que la información es recogida de forma "cruda", esta es analizada por varios sistemas de "filtrado". Echelon es famoso por utilizar un sistema denominado *diccionario*, que no es más que algunas supercomputadoras capaces de encontrar palabras claves dentro de la información

El programa *"Diccionario"* es capaz de almacenar un amplio banco de datos sobre objetivos específicos partiendo de un nombre, una dirección, un número telefónico u otros criterios seleccionados.

Las computadoras de este programa permiten reconocer palabras, teclas, números y hasta timbres de voz, de comunicaciones telefónicas, de fax o de correo electrónico a través de internet. El programa permite interceptar en sólo media hora hasta cerca de mil millones de mensajes, que luego son filtrados para extraer los datos de interés para cada país. Así, la aparición de palabras como "terrorismo", "bombas" o "ántrax" es motivo de alarma. Estas son algunas de las

---

[84] Encryption (encriptación, cifrado) El cifrado es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de dato.
[85] Conectar.
[86] http://news.zdnet.co.uk/story/0,,s2079849,00.html -->

palabras que el programa diccionario tiene como prioridad detectar: ECHELON, UKUSA, NSA, FBI, CIA, NASA, DEA, ETA, KGB, hacker, talibán, Al Qaeda, asesinar, matar, atentado, unabomber, bomba, ántrax comunismo, izquierda, terrorismo, White House, cartel, radicalismo, afgano, George Bush, Osama Bin Laden, Tony Blair, Saddam Housein, Fidel Castro, Cuba, Rusia.[87]

Con la lista de palabras compartida por todas las agencias. Por ejemplo el diccionario de la estación Waihopai en Nueva Zelanda podría buscar palabras claves de su propia lista para la GCHQ de Gran Bretaña, mientras que la estación de Gran Bretaña podría hacer lo mismo para la de Nueva Zelanda.

El filtrado de las conversaciones telefónicas resulta más problemático, porque aún no puede utilizarse un programa para detectar automáticamente palabras verbales. El sistema que se utiliza es la preselección de los números de teléfono y de las identidades fónicas (la huella vocal individual). De todos modos, según las revelaciones de algunos ex agentes británicos, Echelon utiliza modernísimos sistemas de detección de voz capaces de "entender" palabras clave. Al "escuchar" una de estas palabras, graban automáticamente las comunicaciones detallando incluso la posición de emisor y receptor.

Las únicas comunicaciones que resultan relativamente seguras son las que circulan por cable de fibra óptica en el interior de la Unión Europea, debido a su alta capacidad de transporte y la extrema dificultad de seleccionar los mensajes.

Es difícil pensar que existe un sistema que sea capaz de interceptar la información que pasa por internet, pero incluso Echelon en su momento (hace aproximadamente ocho años) era más grande que internet.

---

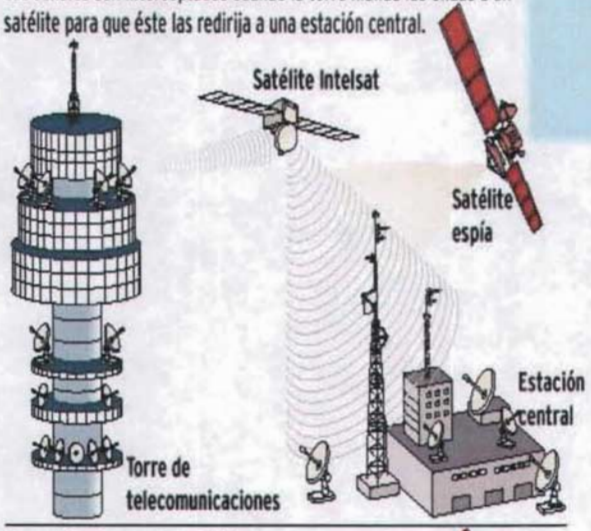
[87] *cfr* http://www.seprin.com/perturba_echelon.htm -->

Echelon, la red espía

Un total de 120 satélites rastrean las comunicaciones de gobiernos, empresas y ciudadanos y las envían al centro neurálgico de Echelon en Fort Meade (Maryland).

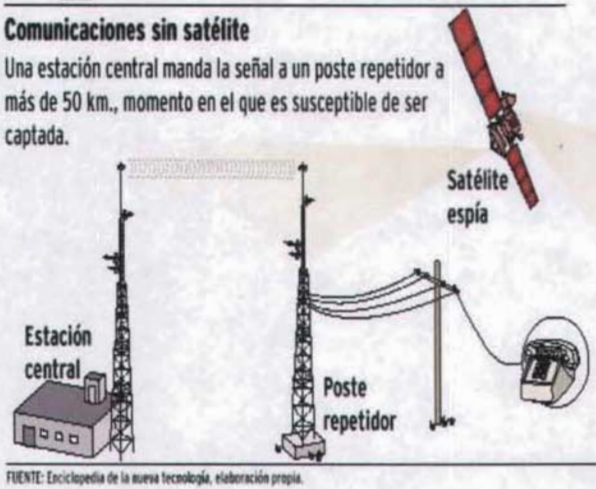
Comunicaciones por satélite

Las señales son interceptadas cuando la torre manda las ondas a un satélite para que éste las redirija a una estación central.



Comunicaciones sin satélite

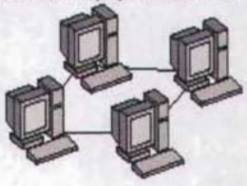
Una estación central manda la señal a un poste repetidor a más de 50 km., momento en el que es susceptible de ser captada.



Centros de recopilación

Internet y correo electrónico

Mediante rastreadores (sniffers), se peina la red en busca de contenidos considerados peligrosos en los paquetes de datos.



Centros de recopilación y procesamiento

La información es procesada en estos centros por potentes ordenadores con diccionarios cargados de palabras clave.

FUENTE: Enciclopedia de la nueva tecnología, elaboración propia.

Mariano Zafra/ EL MUNDO

FUENTE: http://www.seprin.com/echelon27-08-01/echelon.htm -->

2.4 Componentes de Echelon

Sobre los medios de que disponen las agencias implicadas poco se puede decir salvo que están perfectamente capacitadas para realizar tales acciones... acaso tienen escasez de recursos humanos. La NSA tiene un presupuesto anual de unos 4 000 millones de dólares y mantiene bajo su control 120 satélites militares. Sus antenas de recepción cubren la totalidad del planeta. Unos ejemplos de satélites militares son:

"MILSTAR: Programa de los Estados Unidos que gestiona 6 satélites geoestacionarios para la intercomunicación de sus tropas a nivel mundial (bases terrestres, navíos, aviones).

DSCS: 5 satélites que permiten una comunicación global. También de los Estados Unidos.

SKUNET: Sistema británico con cobertura mundial".[88]

Las cifras relacionadas con la composición de esta red son escandalosas. Hay que tener en cuenta además que se trata de una estructura de carácter secreto, por lo que no existen datos oficiales al respecto.

Aún así se han ido descubriendo numerosos datos respectivos a Echelon. Se sabe por ejemplo que dos nodos[89] de la red se encuentran en College Park (Maryland, USA) y Mountain View (California, USA) y pertenecen directamente a la NSA. Otro nodo se situaría en Westminster (Londres, Gran Bretaña). La estación de escucha de Morwenstow (Reino Unido) se encarga de la coordinación de las diferentes escuchas realizadas a los satélites Intelsat de Europa, océano Atlántico y océano Pacífico. Las estaciones de Menwith Hill (Gran Bretaña) y Bad Aibling (Alemania) se encargan de lo mismo, pero de los satélites que no forman parte de la red Intelsat (como los Inmarsat). También se sabe de la existencia de un

[88] http://webs.ono.com/usr016/Agika/6temas_relacionados/echelon.htm
[89] centros de recopilación.

submarino llamado USS Match, encargado de pinchar las comunicaciones por cable submarino.[90]

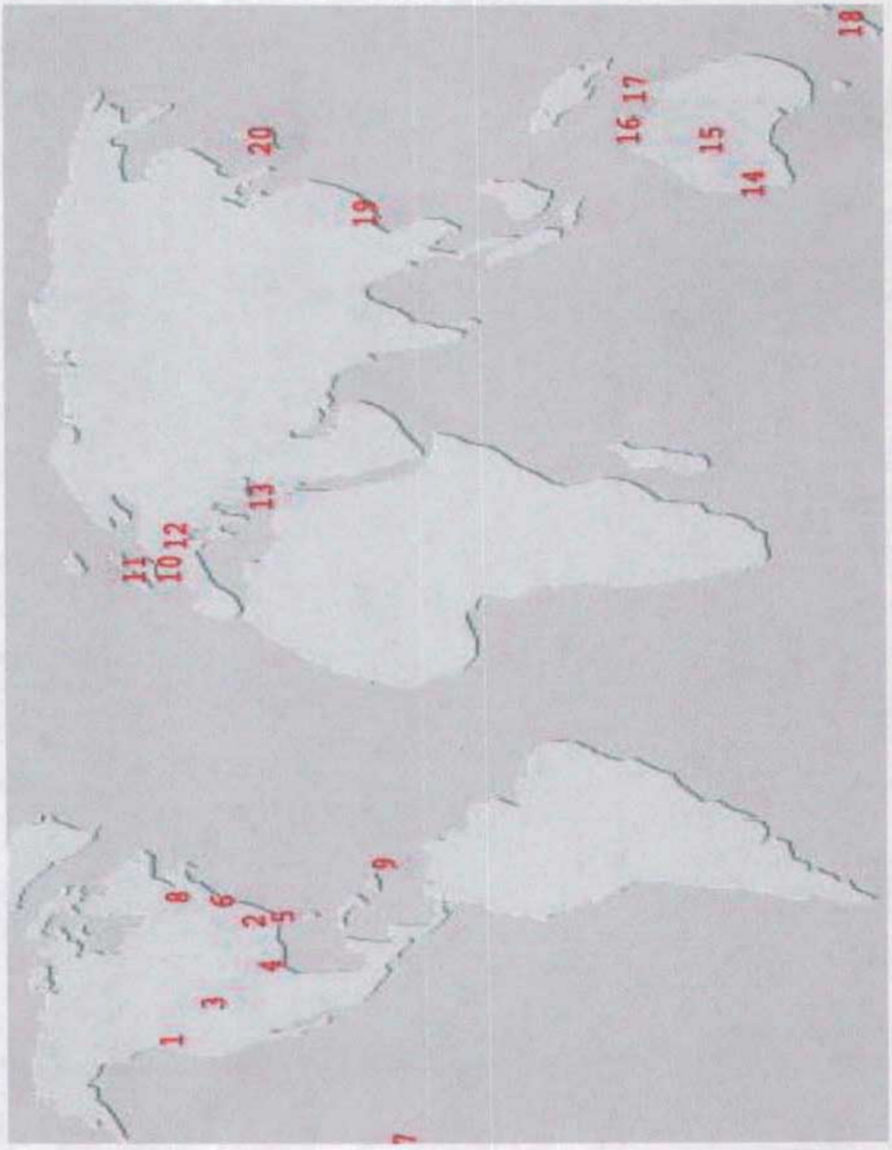
Las más importantes estaciones de rastreo y escucha se sitúan en:

1. Sugar Grove (Virginia, USA)
2. Leitrim (Canadá)
3. Sabana Seca (Puerto Rico, estado asociado de USA)
4. Menwith Hill (Gran Bretaña)
5. Bad Aibling (Base norteamericana en Alemania)
6. Waihopai (Nueva Zelanda)
7. Shoal Bay (Australia)

Alrededor de estas siete centrales se apoyan el resto de las unidades informáticas terrestres, satélites, submarinos y aviones formando una gran red que cubre todo el planeta. También se sitúa el núcleo central del programa informático en la estación antes mencionada de Menwith Hill. "Esta base secreta inglesa está camuflada en una zona rural y allí trabajarían unas 1400 personas."[91]

[90] *cfr* http://webs.ono.com/usr016/Agika/6temas_relacionados/echelon.htm
[91] *Idem*

Veamos el total de las estaciones conocidas:



Fuente: http://webs.ono.com/usr016/Agika/6temas_relacionados/echelon.htm

Lista de estaciones de escucha y localización geográfica.

"1. Yakima (Estados Unidos) 120°O, 46°N

Base del 544° Grupo de Inteligencia (Destacamento 4) de la Air Inteligence Agency (AIA) y del Naval Security Group (NAVSECGRU). Tiene 6 antenas de satélite orientadas hacia los satélites Intelsat del Pacífico y Atlántico. Una de las antenas estaría orientada hacia el satélite Immarsat 2. Se encarga del "Intelligence Support" (apoyo informativo) respecto a la escucha de satélites de comunicación a través de estaciones de la Marina (de Estados Unidos).

2. Sugar Grove (Estados Unidos) 80°O, 39°N

También en esta base se encuentra el NAVSECGRU y el 544° Grupo de la AIA (Destacamento 3). Cuenta con 10 antenas de satélite. Tres de ellas serían mayores de 18 metros.

3. Buckley Field (Estados Unidos) 104°O, 40°N

Dirigida por el 544° IG (destacamento 45). Consta de al menos 6 antenas de las cuales cuatro superan los 20 metros. Oficialmente su cometido consiste en la recopilación de datos sobre acontecimientos en el ámbito nuclear mediante satélites SIGINT (satélites que captan e interpretan señales electromagnéticas), en su análisis y evaluación.

4. Medina Annex (Estados Unidos) 98°O, 29°N

Se trata de otro RSOC (Centro de Operaciones de Seguridad Regional) controlado por el NAVSECGRU y la AIA, cuya área de acción es el Caribe.

5. Fort Gordon 81°O, 31°N

Otro RSOC gestionado por el INSCOM y la AIA (702° IG, 721° IG, 202° IB, 31° IS). Sus cometidos son desconocidos.

6. Fort Meade (Estados Unidos)76°O, 39°N

Es la sede de la NSA (Agencia de Seguridad Nacional de los Estados Unidos).

7. Kunia (Hawai, Estados Unidos) 158°O, 21°N

Gestionada por el NAVSECGRU, el RU y la AIA. Oficialmente es un Centro de Operaciones de Seguridad Regional (RSOC) y tendría como tareas asignadas la preparación de información y comunicaciones así como el apoyo criptográfico. La verdad es que su cometido no está nada claro.

8. Leitrim (Canadá) 75°O, 45°N

Forma parte de un intercambio de unidades entre Estados Unidos y Canadá. Consta de 4 antenas y las dos mayores son de unos 12 metros de diámetro. Oficialmente esta estación se dedica a la "calificación criptográfica" y a la interceptación de comunicaciones diplomáticas.

9. Sabana Seca (Puerto Rico) 66°O, 18°N

Utilizada por el Destacamento 2 del 544° AIA y por el NAVSECGRU. Cuenta con varias antenas, una de ellas de 32 metros. Procesa las comunicaciones por satélite, brinda servicios de criptografía y comunicación y sirve de apoyo a labores realizadas por la Marina y por el Ministerio de Defensa, como por ejemplo recoger informaciones provenientes de los COMSAT. Se supone que se convierta en la más importante estación de análisis y procesado de comunicaciones por satélite.

10. Morwenstow (Inglaterra) 4° O, 51°N

Estación manejada por el GCHQ (Servicio de Inteligencia británico). Cuenta con unas 21 antenas, tres de ellas de 30 metros. No se conoce su cometido especial, pero por su configuración y localización geográfica no cabe duda de que se dedica a la interceptación de comunicaciones por satélite.

11. Menwith Hill (Inglaterra) 2°O, 53°N

Utilizada conjuntamente por Estados Unidos y Gran Bretaña. Por parte de los primeros, se encuentran en la estación el NAVSECGRU, la AIA (45°IOS) y el ISNCOM. La estación pertenece al Ministerio de Defensa británico, que se la alquila a los Estados Unidos. Cuenta con 30 antenas, 12 de ellas con un diámetro superior a los 30 metros. Al menos una de las antenas grandes es una antena de recepción de comunicaciones militares (AN/FSC-78). Su cometido sería proporcionar transmisiones rápidas por radio e investigar las comunicaciones. Así mismo se habla de que, aparte de ser una estación terrestre para satélites espías, se encargaría también de la escucha de los satélites de comunicación rusos.

12. Bad Aibling (Alemania) 12°E, 47°N

Controlada por el NAVSECGRU, el INSCOM (66° IG, 718 IG) y varios grupos de la AIA (402° IG, 26° IOG). Consta de 14 antenas, todas menores de 18 metros. Oficiosamente, se encarga de los satélites SIGINT (espionaje electromagnético) y de las estaciones de escucha de los satélites de comunicación rusos. EL Departamento de Defensa de los Estados Unidos ha decidido cerrar esta estación el 30 de Septiembre del 2002.

13. Agios Nikolaos (Chipre) 32°E, 35°N

Consta de 14 antenas de tamaño desconocido. Controlada por Gran Bretaña en ella trabajan dos unidades: el "Signals Regiment Radio" y la "Signals Unit" de la RAF. Es una estación muy próxima a Oriente Medio y es la única estación de esa zona de huellas de satélite.

14. Geraldton (Australia) 114°E, 28°S

Se encarga de ella el DSD (Servicio Secreto australiano) si bien los agentes británicos que se encontraban en Hong Kong hasta que esta ciudad pasó a formar parte de China ahora trabajarían en esta estación australiana. Cuenta

con 4 antenas de 20 metros orientadas hacia el Océano Índico y el Pacífico Sur. Se ocuparía de la interceptación de satélites civiles.

15. Pipe Gap (Australia) 133°E, 23°S

Manejada por el DSD. Sin embargo la mitad de las 900 personas que trabajan allí son de la CIA y del NAVSECGRU. Posee 18 antenas de satélite de las cuales una es de 30 metros y otra de 20 metros. Es una estación para satélites SIGINT desde la cual se controlan varios satélites de espionaje cuyas señales se reciben y procesan. El tamaño de las antenas hace suponer que también se realizan interceptaciones de comunicaciones por satélite pues para los satélites SIGINT no es necesario el uso de grandes antenas.

16. Shoal Bay (Australia) 134°E, 13°S

Estación dependiente del Servicio de Inteligencia Australiano. Posee 10 antenas de tamaño no especificado aunque las más grandes podrían no sobrepasar los 8 metros de diámetro. Las antenas estarían orientadas hacia los satélites PALAPA indonesios. No está claro si forman parte o no de la red mundial de espionaje.

17. Guam (Pacífico Sur) 144°E, 13°S

Controlada por la 544° IG de la AIA y por la Marina de Estados Unidos. Alberga una estación naval de ordenadores y telecomunicaciones. Tiene 4 antenas, dos de ellas de unos 15 metros.

18. Waihopai (Nueva Zelanda) 173°E, 41°S

Estación controlada por el GCSB (General Communications Security Bureau de Nueva Zelanda). Consta de dos antenas, una de ellas de 18 metros. y sus funciones son la interceptación de comunicaciones por satélite y el procesado y descifrado de las transmisiones. Su pequeño tamaño y radio de

acción (una pequeña parte del Pacífico) avala la hipótesis de una intercomunicación complementaria con la estación de Geraldton (Australia).

19. Hong Kong 22°N, 114°E

No se disponen de datos exactos referentes ni a su tamaño ni a su número de antenas. Sin embargo se sabe que posee varias antenas de gran diámetro. Tras la incorporación de Hong Kong por parte de China la estación fue suprimida. No se sabe cual de las estaciones cercanas ha asumido el papel que desempeñaba la estación de Hong Kong (Geraldton, Pipe Gap, Misawa,...). Parece ser que dichas labores se repartieron entre varias estaciones.

20. Misawa (Japón) 141°E, 40°N

Controlada por Estados Unidos y Japón. Consta de 14 antenas, algunas de ellas de 20 metros. Es un centro de operaciones de criptología (Cryptology Operations Center) e intercepta las señales de los satélites rusos Molnyia y de otros satélites de comunicación también rusos."[92]

2.5 Denuncias a la red Echelon

A la Red Echelon se le atribuyen, entre otras, estas acciones de carácter comercial y político:

- *"Interceptación y escucha de transmisiones de Greenpeace por parte de los Estados Unidos durante su campaña de protesta hacia las pruebas nucleares francesas en el Atolón de Mururoa en 1995. Este espionaje no fue conocido por sus socios más débiles, como Nueva Zelanda y Australia.*

[92] http://webs.ono.com/usr016/Agika/6temas_relacionados/echelon.htm -->

- *Espionaje a dos ministros británicos por parte de Margaret Thatcher, siendo ella Primera Ministra del Reino Unido.*

- *Espionaje del diario Observer y a varios de sus periodistas y propietarios.*

- *La inteligencia militar francesa asegura que agentes secretos norteamericanos trabajan en la empresa Microsoft (lo que faltaba) para instalar programas secretos en los productos e indicar a los desarrolladores de programas de Microsoft qué agujeros de seguridad deben crear para que la NSA pueda entrar a través de ellos. Estos agujeros de seguridad se encuentran en productos como Windows e Internet Explorer. A cambio, recibiría apoyo financiero y se favorecería el monopolio del Microsoft en el mercado nacional e internacional, lo cual beneficia a ambas partes.*

- *Se asocia a la NSA la inclusión del denominado "cifrado fuerte" del Windows 2000 para fines tan desconocidos como preocupantes.*

- *Los sistemas de encriptación de mensajes de los productos Microsoft, Netscape y Lotus destinados al mercado europeo son distintos a los americanos y están predispuestos a ser decodificados los la NSA.*

- *La empresa informática Lotus reconoce que la NSA obliga a las empresas americanas a comunicarles una parte de la clave de codificación de los productos destinados al intercambio de mensajes que se exporten fuera de los Estados Unidos. En su caso, 24 de los 64 bits del código de desencriptación de los mensajes.*

- *La empresa suiza Crypto AG, expertos en programas, hardware y otros productos criptográficos (teléfonos móviles, por ejemplo) adjunta a los mensajes enviados a través de sus productos una clave de decodificación del password utilizado por el usuario que conocería la NSA. Se sabe que dicha empresa suiza y la NSA vienen manteniendo contactos y reuniones desde hace unos 25 años. Los productos Crypto son utilizados por delegaciones oficiales de más de 130 países, tales como ejércitos, embajadas, ministerios,... Parece ser que aún seguimos sin poder fiarnos de los suizos... que se lo pregunten a los judíos.*

- *Interceptación de comunicaciones entre Thomson-CSF y el Gobierno Brasileño en 1994 en la negociación de un contrato de 220.000 millones de pesetas para un sistema de supervisión por satélite de la selva amazónica permitió la concesión del proyecto a la empresa norteamericana Raytheon, vinculada a las tareas de mantenimiento de la red Echelon.*

- *Interceptación de faxes y llamadas telefónicas entre Airbus y el Gobierno de Arabia Saudí con detalles de las comisiones ofrecidas a los funcionarios permitió a Estados Unidos presionar para que el contrato de un billón de pesetas fuera concedido a Boeing-McDonnell Douglas. 1995.*

- *Espionaje a la industria automovilista japonesa.*

- *Intercepción de la NSA de comunicaciones entre el Gobierno de Indonesia y representantes de la empresa japonesa NEC referentes a un contrato de 200 millones de dólares en equipamiento de telecomunicaciones. George Busch padre intervino personalmente y obligó a Indonesia a dividir el contrato entre NEC y la firma estadounidense AT&T (proveedora de equipamiento de telecomunicación a la NSA).*

- *Espionaje a las conversaciones entre países de Oriente Medio y representantes del consorcio europeo Panavia destinadas a la venta del cazabombardero Tornado a dichos países."*[93]

En Argentina también hay serios rumores sobre intervenciones de comunicaciones.

Un ingeniero de telecomunicaciones habría detectado que 21 líneas de teléfono del Ministerio de Economía de Argentina estaban siendo pinchadas desde el exterior, vía satélite. Se realizaron entonces revisiones de las líneas de teléfono del ministro y varios secretarios del ministerio. En estas revisiones se descubrió que todos los teléfonos pinchados lo estaban a través de una computadora del mismo ministerio marca AST (empresa informática norteamericana que abastece a la NSA de equipamiento). Investigando la computadora en cuestión se descubrió que tenía instalado un software denominado STG, el cual permite la intervención de líneas de fibra óptica, cable, teléfono, correo electrónico, fax y satélite.

El sistema basado en el software STG incluye un dispositivo de seguridad que es revisado y actualizado cada 24 horas por el mismísimo Departamento de Estado norteamericano y para que el programa se mantenga activo, debe conectarse con el Pentágono cada día. Este software sólo puede ser adquirido por organismos autorizados por el Departamento de Estado de los EE.UU. En Argentina, el único organismo autorizado es la SIDE (Secretaría de Inteligencia del Estado). Sin embargo, se comprobó que el pinchazo provenía del exterior de Argentina en una conexión vía satélite.

La lucha contra la red Echelon ha llegado también al ciudadano promedio y se ha creado un virus informático específico para esta red de

---

[93] http://webs.ono.com/usr016/Agika/6temas_relacionados/echelon.htm -->

espionaje llamado SEPRIN. Se trata de un virus que intentaría saturar los recursos de la misma.[94] Su efectividad aún no ha sido demostrada.

2.6 Agencia Nacional de Seguridad (NSA)

Fuente: www.nsa.gov

La Agencia Nacional de Seguridad es la organización criptologica de los Estados Unidos de América. Coordina, dirige, y realiza las actividades altamente especializadas para proteger los sistemas de información norteamericanos y se encarga de obtener información de origen extranjero. Además de trabajar conjuntamente con otras agencias de inteligencias del mundo. La National Security Agency cuenta con más de 38000 empleados y 4000 millones de dólares de presupuesto y es la agencia estadounidense que lidera el proyecto llamado ECHELON.

[94] *cfr* http://www.seprin.com/virus_logico.htm

La NSA es una organización con alta tecnología de punta. La NSA está en las fronteras de comunicaciones y proceso de datos. También es uno de los centros más importantes del análisis del idioma extranjero e investigación dentro del gobierno estadounidense.

El NSA dirige los principales programas de investigación de los EEUU. Algunos de sus proyectos han significado grandes avances en el mundo de la ciencia y del comercio.

El interés temprano del NSA en la investigación de "cryptanalytic," los condujo a llevar esta tecnología a la primera computadora de gran potencia y la primera computadora transistorizada, los predecesores a la computadora moderna. NSA abrió el camino para desarrollar las unidades de almacenamiento flexibles que condujo al desarrollo de la cinta de cassette. NSA también hizo estudios de irregularidades del suelo terrestre desarrollando la tecnología del semiconductor y continúa siendo un líder mundial en muchos campos de la tecnología.[95]

La NSA emplea una serie de códigos para obtener información, estos códigos son denominados *codemakers y codebreakers* que son algo así como los códigos con la información más importante del país. Para esto cuentan con el patrón más grande de matemáticos en los Estados Unidos y quizás del mundo. Sus matemáticos contribuyen directamente en dos misiones de la NSA: diseñan programas que protegen la integridad de los sistemas de información de los Estados Unidos y buscan las debilidades de otros sistemas adversarios.

La tecnología evoluciona rápidamente, es inaceptable que países como EEUU se queden rezagados y ver como otras naciones dominan la tecnología de punta. El actual contexto internacional exige poner énfasis en los retos

[95] cfr. Business Week, 05/31/99 Issue 3631, p110

tecnológicos. La National Cryptologic School es indicativa del compromiso de la NSA en el desarrollo profesional. La escuela no sólo proporciona el único entrenamiento para la mano de obra de la NSA sino que también sirve como un medio de entrenamiento para todo el Departamento de Defensa. La NSA apoya a sus empleados para terminar sus estudios dentro de las mejores universidades y colegios del país y selecciona a sus mejores empleados para que asistan a "colegios de guerra" de las Fuerzas Armadas Americanas.[96]

La mayoría de los empleados del NSA, ya sean civiles o militares son encuartelados en el Fuerte Meade, Maryland, localizado entre Baltimore y Washington DC. Su mano de obra representa una combinación inaudita de especialidades: analistas, ingenieros, físicos, matemáticos, lingüistas, ingenieros en computación, investigadores, así como especialistas de relaciones públicas, oficiales de seguridad, administradores, gerentes, secretarios y asistentes clérigos.

Las señales extranjeras de inteligencia o SIGINT permiten una organización eficaz, unifica de todas las señales extranjeras y de los EE.UU. NSA esta autorizado para producir SIGINT de acuerdo con los objetivos, los requisitos y prioridades de los EEUU.

La Agencia de Seguridad Nacional (NSA) realiza la vigilancia electrónica para coleccionar la información de inteligencia extranjera para el ejército y políticos. NSA proporciona valiosa información al gobierno estadounidense así como información de importancia a los ciudadanos, como el terrorismo internacional, narcotráfico, y proliferación de armas de destrucción de masiva. Las actividades de vigilancia electrónicas de la NSA también están sujetas a la vigilancia de múltiples comisiones, áreas y secretarías del gobierno estadounidense. Estos "resguardos" han asegurado que la NSA este operando dentro de un marco legal.

---

[96] *cfr* http://www.nsa.gov/about_nsa/index.html -->

CAPÍTULO 3

ECHELON EN EL DERECHO INTERNACIONAL

3. Echelon en el derecho internacional

Existen diversos instrumentos jurídicos a nivel internacional, (tratados, constituciones, convenios) los cuales protegen la privacidad, pero estos instrumentos jurídicos no protegen la privacidad en su totalidad, sólo abarcan algunos aspectos de la privacidad ya sea en correspondencia, en internet, o en llamadas telefónicas.

El único instrumento internacional efectivo que garantiza la protección de la privacidad es el *European Convention on Human Rights*, que como se verá más adelante es tan amplio que su alcance incluye internet. Aunque su campo de acción sólo es aplicable obviamente en Europa.

A pesar de la existencia del *European Convention on Human Rights,* los principales afectados por Echelon (ONG´s, Estados, empresas transnacionales) están consientes de la necesidad de crear un marco jurídico a nivel internacional que regule esta disyuntiva, es decir, un instrumento en que todos los afectados por la red mundial de espionaje Echelon puedan resguardarse ante la violación de sus derechos por parte de esta red.

Sin embargo, existen afirmaciones sobre la improbabilidad de que los integrantes del pacto UKUSA se apeguen a un instrumento jurídico internacional que limite o pare sus actividades de espionaje en todo el mundo y menos en estos tiempos donde la seguridad nacional parece ser un una directriz a seguir por parte de los países que conforman la red Echelon.

3.1 El individuo y el Estado

Gobiernos y organizaciones del sector público y privado han ido avanzando en años recientes hacia la inclusión de la vigilancia en casi todas nuestras actividades personales como finanzas, comunicaciones y forma de vida. Mientras se alaba la privacidad de boca para fuera, se argumenta que la vigilancia es necesaria para mantener la ley y el orden y para conseguir eficacia económica. La justificación es a menudo interesada y algo falsa, pero una cantidad fundamental de personas han sido persuadidas, no obstante, de que la renuncia a la intimidad es el precio que hay que pagar por una sociedad supuestamente mejor y más segura.

La cuestión no ha sido nunca sencilla. La protección de la privacidad individual ha sido siempre una de las grandes polémicas de los derechos humanos. En su centro se encuentra la lucha por encontrar el equilibro ideal entre la autonomía del individuo y el poder del Estado.

Esta lucha por el equilibrio se desarrolla cada día de mil maneras. Con cada nueva intromisión en la vida privada –ya sea Televisión en Circuito Cerrado (TVCC), o vigilancia del correo electrónico -- la gente se ve obligada a elegir entre sus derechos individuales y los derechos de la sociedad.

Sin embargo, aunque el problema es más complejo de lo que jamás ha sido, también es más urgente que nunca. Probablemente, nunca ha habido un momento en la historia en el que se haya acumulado tanta información sobre la población en general. Los detalles de un adulto medio económicamente activo, del mundo desarrollado, se encuentran en cerca de 400 de las principales bases de datos: suficiente información procesada como para recopilar un enorme

historial de cada persona.[97] La vigilancia visual electrónica en los centros urbanos es ya omnipresente.[98] Prácticamente todas las formas de comunicación electrónica se exploran y analizan ya rutinariamente.

Estas actividades han dado lugar a un sector económico floreciente. En países como Gran Bretaña, Estados Unidos, Francia la industria de vigilancia en todas sus formas (investigadores privados, agencias de crédito, servicios de seguridad, etc.) emplea a más de un millón de personas por país, tal población de fisgones profesionales se explica, en parte, por la aparición de la vigilancia de masas. En el pasado, la vigilancia apuntaba a individuos o grupos específicos perfectamente detectados, ahora la vigilancia sistemática en un número creciente de ámbitos analiza activamente a millones de personas a la vez no importando a lo que se dediquen.

Tradicionalmente, la reacción pública a la invasión de la intimidad ha sido contradictoria e impredecible. Aunque las encuestas de opinión muestran consistentemente que la gente se preocupa por su intimidad, es cierto que otro sector esta a favor a la violación de su intimidad sí esta garantiza la seguridad de la sociedad y por ende la suya.

En los Estados Unidos, la toma de huellas digitales a los cobradores de la beneficencia social ha proseguido con un escaso murmullo de protesta mientras que, en Australia, los intentos del gobierno federal de introducir una tarjeta nacional de identidad provocaron en los años ochenta las mayores protestas públicas que se recuerdan en ese país. Sin embargo, mientras la legislación australiana que obliga a los bancos a informar de las transacciones sospechosas pasó sin llamar la atención, leyes similares en los Estados Unidos provocaron más de un cuarto de millón de quejas por escrito. En Alemania y Australia, las propuestas de introducir servicios de telefonía digital desataron una amplia

[97] *cfr* Simos Davies *La privacidad en la encrucijada.* p.34
[98] En las calles, centros comerciales, oficinas, aeropuertos.

preocupación por la intimidad. Idéntica tecnología fue introducida en Gran Bretaña con escasa o nula discusión.[99]

3.2 La privacidad como derecho humano

Causa o efecto, la privacidad ocupa ahora un lugar poco envidiable en el catálogo de los derechos humanos. Junto a la censura y la libertad de expresión, la privacidad sigue siendo una polémica compleja, y su solución un desafío. Durante el último cuarto de siglo, ningún otro derecho fundamental en el ámbito de la política pública ha generado tanta turbulencia y controversia. "*La privacidad es el derecho del cual todos los demás se derivan*"[100]. "Es el centro de la libertad y autonomía del pueblo y es, tal vez, el factor clave que limita el poder del Estado."[101]

Tortura, discriminación, terrorismo, odio racial: todas estas cuestiones han conseguido un consenso básico en la comunidad internacional. La privacidad, sin embargo, es percibida por muchos gobiernos y corporaciones como el problema de los derechos humanos. Es común para muchas organizaciones el que la privacidad y la protección de la información personal impiden el rendimiento económico y la aplicación de las leyes. El resultado es que muchos países se están convirtiendo en sociedades vigiladas. La justificación es seductora y difícil de contrarrestar. Y en nuestro inocente y natural deseo de ahorrar un poco de dinero, o simplemente de ser buenos ciudadanos, cedemos constantemente información acerca de nuestra vida personal: como finanzas, compras, empleo, intereses, actividad telefónica, e incluso nuestros desplazamientos geográficos. Inevitablemente, cuando así lo hacemos, las

---

[99] *cfr* Simos Davies *La privacidad en la encrucijada.* p.35
[100] *Ibidem* p 38
[101] *Ibidem* p.39

organizaciones están listas para explotar esos datos. La vigilancia se ha convertido en un componente fijo de la próspera economía de la información además de ser habitual en nuestras vidas, aunque no nos demos cuenta de ello.

Es ya un escenario común que la potencia, capacidad y velocidad de la tecnología de la información se están acelerando rápidamente. El alcance de la invasión de la privacidad (o al menos el potencial para invadirla) crece a la par. Pero no es sólo la acrecentada capacidad y el costo decreciente de la tecnología de la información lo que genera amenazas a la privacidad. La globalización de sistemas como internet elimina las limitaciones geográficas (y las protecciones legales) al flujo de los datos. La tendencia está conduciendo a la eliminación de las barreras tecnológicas entre sistemas. Los modernos sistemas de información tienen una creciente capacidad de interacción con otros sistemas y pueden intercambiar mutuamente y procesar diferentes clases de datos, es decir, todo se esta haciendo compatible con todo no importando para que fin. Entretanto, el fenómeno multimedia, que funde varias formas de transmisión y expresión de datos e imágenes, crea enormes dificultades a los legisladores que desean proteger la intimidad personal.

Recientemente, la cadena de televisión BBC[102] presentó un documental sobre la privacidad[103], en el que describía uno de los resultados imprevistos de estas macro tendencias de la tecnología: una compañía de Gran Bretaña llamada *InfoDisc*, había producido un CD-ROM que cruza los datos de las listas electorales con los de la guía telefónica y datos geodemográficos. Así, la más elemental e inocente información acerca de usted puede ser introducida en el disco, revelando toda clase de hechos. Su número de teléfono lleva instantáneamente a su dirección. Su nombre lleva automáticamente a su profesión y edad. No es necesario decir que los sectores de finanzas y créditos,

[102] British Broadcasting Corporation (BBC), primera, pionera y mayor compañía de radiodifusión del Reino Unido, y una de las mayores del mundo.
[103] *El derecho a la privacidad*, presentado por Beatriz Gómez, Sección Latinoamericana de la BBC.

investigadores privados, periódicos, empresas de mercadotecnia y policía hacen uso intensivo de este producto.

Estas cuestiones son importantes porque el creciente lazo de información entre el ciudadano y el Estado (y el sector privado, naturalmente) disminuye la autonomía humana. Conforme se automatiza la toma de decisiones por las instituciones, los factores que afectan a nuestras vidas se construyen sobre la base de una masa creciente de datos personales íntimos. Poco a poco, las decisiones personales las van tomando un grupo de gobernantes, políticos y/o empresarios argumentando que están haciendo la vida del individuo más practica, más fácil y más rápida.

3.3 Derecho a la privacidad

"Para el derecho anglosajón, la privacidad (privacy) es el derecho que tiene una persona de no ser molestada o sufrir invasión a su persona o a su información personal, así como a sus relaciones y comunicaciones privadas, entre las que se cuentan las comunicaciones electrónicas."[104]

Es un hecho que al lado de toda la magia que brindan las nuevas tecnologías de la información, también presentan cuestiones *obscuras*: en este caso, representan un serio riesgo para la privacidad.

La privacidad (*privacy*) es un concepto producto de la influencia del derecho anglosajón, aunque su esencia es una cuestión jurídica contemplada y protegida como garantía individual, dentro de los conceptos de derecho de igualdad, libertad y seguridad jurídica en prácticamente todo el mundo. Como

[104] http://www.assemblee-nationale.fr/2/2textes-a.html

se mencionaba anteriormente el término, *privacy* constituye un bien jurídico con proyección social, que muestra el ejercicio de la libertad humana y, asimismo, impone un límite en las relaciones sociales.

"El atentado al derecho a la intimidad (en el marco de las garantías individuales) como problemática que plantea el derecho tecnológico y la aplicación de las tecnologías de la información, es un fenómeno que debemos enfrentar a partir de nuestra realidad, toda vez que la reivindicación de los derechos humanos ha variado de manera singular. Ese universo conceptual y contextual se ha visto modificado por la transformación de los presupuestos antropológicos y cosmológicos que se han producido en nuestras sociedades tecnológicas."[105]

Es importante destacar que, en materia de internet, el proveedor del servicio, el dueño de una base de datos (bancos, compañías de tarjetas de crédito, empresas de telemarketing, oficinas de gobierno, por nombrar sólo algunas) debe permitir a toda persona verificar y, de ser necesario, corregir cualquier información sobre ella. Asimismo, una persona puede prohibir el uso de su información personal en una base de datos. En un futuro cercano, debe haber mayor garantía de empresas y proveedores de acceso a internet para que el carácter confidencial del a información personal se respete. En el terreno de internet es necesario que el proveedor del servicio dote al usuario de programas o alguna clase de solución que impidan el libre espionaje de archivos en la computadora del navegante y no me estoy refiriendo solamente al espionaje que pueda realizar Echelon, ya que el usuario puede ser espiado por un simple aficionado que guste por intrometerse en las computadoras de los demás. Es urgente una regulación de este derecho fundamental a fin de proteger la llamada información personal, es decir, la integrada por datos personales. Así se

---

[105] Gabriela Barrios Garrido, *Internet y derecho en México*. Ed. McGraw-Hill, México, 1998, p. 47

reconocería explícitamente la obligación que tiene el Estado y el resto de la sociedad al respeto a la vida privada del ser humano.

"El derecho mexicano no ha reglamentado esta garantía individual que se deduce de las libertades de la persona en el aspecto espiritual, a saber, la libertad de intimidad (artículo 24 constitucional), que comprende dos aspectos: inviolabilidad de correspondencia (articulo 25 constitucional) e inviolabilidad del domicilio (artículos 16 y 26 constitucionales)."[106]

Con el propósito de garantizar jurídicamente el derecho de la privacidad, toda persona requiere de mandamiento judicial escrito, fundado y motivado para ser molestado en su persona, familia, domicilio, papeles, o posesiones. Es decir, no puede violarse la intimidad de ningún individuo sin un mandamiento judicial escrito, conforme a derecho y con fundamento en la ley. Lamentablemente, la realidad, muestra que este derecho, por falta de regulación, es uno de los menos respetados y olvidados, tanto por violaciones del orden común como de la misma autoridad. Incluso ya parece ser de lo más común violar este derecho.

"Así, el papel que juegan los sistemas de telecomunicación frente a los derechos humanos es dual, ya que, por un lado, la informática se constituye en un instrumento capaz y eficiente para hacer respetar estos derechos y, por el otro, representa la herramienta más amenazante de la sociedad contemporánea para aniquilarlos."[107]

Y es esta una de las disyuntivas acerca de este tema: el sacrificar la privacidad del individuo a cambio de ofrecer seguridad, (que no sabemos cuanta ni que tan certera sea) ávida en nuestros tiempos. Y es que el Estado que es el que provee la seguridad tiene la intención de sacrificar la privacidad de

[106] *Ibidem* p. 48
[107] *Idem*

una sociedad a cambio de garantizar seguridad, pero al parecer el individuo (obvio) no esta dispuesto a sacrificar su privacidad.

"Las redes de comunicación informáticas unen al mundo en segundos; las fronteras físicas y temporales forman parte del pasado. Louis Darms señaló en 1980 que la mayoría de los no participantes del poder consideraban la interconexión de computadoras, bajo la óptica de una subdivisión de poderes, el arma absoluta del dictador. También afirmó que la revolución tecnológica de la telemática constituiría la primera oportunidad concreta para poner "en jaque" el maquiavelismo hereditario de los poderes, ya que suprimiría la visión de superioridad entre dirigentes y dirigidos. Las redes de comunicación se concebían entonces como el arma policíaca más indiscreta e indecente, pues se reservaba a los poderes establecidos el exclusivo derecho de acceso y consulta a los bancos de información, hecho que evidenciaba la superioridad del poderoso." [108]

El respeto y reconocimiento a la vida privada refleja la evolución de las costumbres y hábitos de una sociedad, ya que expresa con precisión la idea que uno tiene del hombre y sus relaciones con el entorno. El respeto al secreto individual y a la privacidad está ligado al progreso y al respeto de los derechos del hombre en una comunidad. De hecho, todas las reflexiones jurídicas, sociales o económicas contemporáneas acaban por invocar la vieja razón de ser del Estado: la protección y respeto al ser humano.

Frente al poder informático, la idea del secreto debe consagrar, en los diversos ordenamientos jurídicos, la libertad de cada individuo a mantener secreta, por razones o necesidades de diversa índole, aquella esfera íntima que ha tenido que hacer del conocimiento de otra persona.

---

[108] *Ibidem* p. 49

No obstante, a pesar de las diversas regulaciones penales en diferentes legislaciones sobre todo europeas, en la práctica el espacio de la vida privada es ciertamente débil por no decir casi nula.

Las nuevas tecnologías de la información han dado un giro a las relaciones humanas, pues presentan a la información como solución normativa de las relaciones entre la sociedad y las formas más comunes de comunicación. Creando una dependencia con la tecnología más común, es decir, todos sabemos utilizar el teléfono o internet, dependemos de de ello en gran medida. Esta figura jurídica reafirma su carácter de derecho social público y se proyecta como un derecho esencial para la sociedad tecnología.

En el mundo contemporáneo, el derecho a la intimidad se confunde en el campo de lo civil y el de lo penal, traduciéndose en la garantía de inviolabilidad domiciliaria y en el secreto de las comunicaciones, pero sin que en tales garantías se comprenda la verdadera naturaleza e implicaciones que reviste el uso abusivo de los datos informáticos.

La información, de cualquier tipo, es necesaria para determinar políticas, tanto en el sector público como en el privado. De ahí la utilidad de la captura, almacenamiento y difusión de la información personal en los bancos de datos. En este contexto, la privacidad informacional se presenta como una gran necesidad. La vida privada no puede definirse en lo especial ni en lo físico; bajo este entorno, la *vida íntima* obtiene una nueva dimensión. De la protección de la información personal deviene, en sí, un problema independientemente de los diversos aspectos de la libertad personal.

El concepto informático de privacidad no está basado en la idea de que el hombre puede replegarse dentro de su esfera privada. La base jurídica es más

amplia, es el derecho de la persona a conservar su autonomía, su identidad y su autodeterminación informativa.

El concepto de vida privada, en relación con la informática y la telemática, tiene un doble significado. Por un lado, la protección de la vida privada, se refiere al problema de la información sensible, definida como aquella relativa al origen racial, a las opiniones publicas, religiosas y membresías sindicales, información que no puede ser recopilada ni procesada electrónicamente salvo que exista autorización expresa del interesado; por el otro lado, el manejo y registro de otro tipo de información puede también causar atentados a la vida privada, pero en relación con el ámbito social al que pertenece.

Como quiera que sea lagunas como estas son aprovechadas por redes de espionaje como Echelon para llevar sus actividades de espionaje sin la más mínima preocupación legal. Por lo tanto, es urgente revisar y reglamentar esta materia a nivel internacional, tomando como marco de referencia regulaciones precisas. La Convención Europea para la protección de personas sobre el tratamiento automatizado de datos de carácter personal, firmado en Estrasburgo el 28 de enero 1981, expresa, en primer término, que su objetivo es *"garantizar, sobre el territorio de cada parte, a toda persona física, cualquiera que sea su nacionalidad o su residencia, el respeto de sus derechos y de sus libertades fundamentales, en particular el derecho a su vida privada, en relación con el tratamiento automatizado de la información de carácter personal" (articulo 1).*[109]

En el tema de internet es necesario reconocer su importancia como un nuevo medio de comunicación de tecnología avanzada. Además, debe fomentarse la defensa del derecho de autodeterminación informática a través de:

---

[109] **PARLAMENTO EUROPEO,** Comisión Temporal sobre el Sistema de Interceptación Echelon p. 8.

1- El reconocimiento de que cada individuo tiene derecho a acceder a la información personal que le afecte, especialmente la de bancos de datos informatizados.

2- El reconocimiento de que cada individuo tiene derecho a controlar, de manera razonable, la transmisión de la información personal que le afecte.

3- Para garantizar el derecho a la intimidad individual las leyes deben regular la limitación de tiempo en que deba conservarse la información personal en la base de datos; la definición de los objetivos de uso de esa información en el inicio de procesamiento de datos; garantizar la calidad de los datos personales, veracidad, integridad y actualidad, y la prohibición de la revelación de datos personales.

3.4 La protección a la privacidad bajo los convenios internacionales

Cualquier acto que involucra la interceptación de comunicaciones, e incluso la grabación de datos por algún tipo de organización de carácter público o privado, representa una seria violación a la privacidad de un individuo (exactamente como lo hace Echelon). Sólo en una *situación policíaca* la interceptación de comunicaciones sin restricción es permitida por las autoridades gubernamentales.[110] En los Estados miembros de la Unión Europea, los cuales cuentan con democracias maduras, el derecho a la privacidad se circunda en las constituciones nacionales de cada miembro. De esta manera la privacidad cuenta con especial protección: las violaciones a los derechos de cualquier

[110] Reporte sobre la existencia de un sistema global para la interceptación de comunicaciones comerciales y privadas (ECHELON interception system) (2001/2098(INI)) p. 83

índole y de carácter potencial son autorizadas sólo siguiendo el análisis de las consideraciones legales y de acuerdo con el principio de proporcionalidad.

Muchos acuerdos bajo la ley internacional especifican el respeto a la privacidad como un derecho fundamental.[111]La problemática aquí radica en que no son respetados, ni siquiera son contemplados por quienes llevan a cabo el espionaje, es como si no existieran.

A nivel mundial, debe hacerse una mención particular al Convenio Internacional sobre Políticas y Derechos Civiles[112], el cual fue adoptado por la ONU en 1966. El artículo 17 del Convenio garantiza la protección de la privacidad.

3.4.1 Declaración Universal de los Derechos Humanos

La Declaración Universal de los Derechos Humanos, proclama los derechos personales, civiles, políticos, económicos, sociales y culturales del hombre, los cuales sólo se ven limitados por el reconocimiento de los derechos y libertades de los demás, así como por los requisitos de moralidad, orden público y bienestar general.

La Declaración Universal de los Derechos Humanos, suscrita por todos los países del acuerdo UKUSA especifica en su artículo 12 que:

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".[113]

---

[111]Articulo 12 de la Declaración Universal de Derechos Humanos; Articulo 17 del Convenio Internacional Sobre Políticas y Derechos Civiles.
[112] Adoptado por la Asamblea General de la ONU el 16 de Diciembre de 1966.
[113] http://www.derechos.org/nizkor/ley/dudh.html -->

3.4.2 *Convenio Europeo de Derechos Humanos*

El objetivo que se propone consiste en alcanzar la protección, mediante la articulación de mecanismos jurídicos eficaces, de los derechos civiles y políticos de los individuos.

El artículo 8 del Convenio Europeo de Derechos Humanos refleja la misma posición, con algunas reservas:

"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".[114]

3.4.3 *Convenio Internacional Sobre Políticas y Derechos Civiles*

También es conocido como Pacto Internacional de Derechos Civiles y Políticos.[115] Este Pacto reconoce los derechos que derivan de la dignidad de la persona humana, así como crear condiciones que permitan a cada persona gozar de sus derechos civiles y políticos, tanto como de sus derechos económicos, sociales y culturales

El artículo 17 especifica que:

"Nadie será sujeto arbitraria o ilegalmente con la interferencia de su privacidad... y que...cada uno tiene derecho a la protección de la ley en contra de tal interferencia..."[116]

---

[114] Dr Chris Elliott, *The legality of the interception of electronic communications*,, p.4
[115] Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966.
[116] Dr Chris Elliott, The legality of the interception of electronic communications, p.4

3.5 Telecomunicaciones internacionales

"En la década de los ochenta, tanto el personal como los visitantes que accedían al bloque de operaciones del Edificio 600, perteneciente a la RAF de Chicksands – una estación de escucha de las fuerzas aéreas estadounidenses situada en Inglaterra– habían de pasar por una puerta de torniquete y un control de seguridad antes de toparse con una broma interna de SIGINT: pegada a la pared había una copia del Convenio Internacional de Telecomunicaciones. El Convenio, ratificado tanto por el Reino Unido como por los Estados Unidos, declara que los Estados miembros protegerán la intimidad de las telecomunicaciones. Los operadores que pasaban por allí se disponían a hacer precisamente lo contrario."[117]

Esta anécdota que al parecer tiene tintes graciosos pone en evidencia el eterno problema de la vigilancia de los servicios de inteligencia, esto es, que su actuación se relaciona automáticamente con la infracción de la ley. La creciente publicidad y la atención prestada a este tema plantean una fuerte investigación, así como una seria revisión al derecho internacional que protege la intimidad de las comunicaciones internacionales y el modo de ejercerlo. SIGINT, que vulnera ampliamente el derecho a la intimidad de las telecomunicaciones, sigue estando fuera del alcance de la mayoría de las jurisdicciones nacionales de cada país afectado.

Dos tratados internacionales protegen las telecomunicaciones internacionales. El primero es el Convenio Internacional de Telecomunicaciones (CIT), por el que se establece la Unión Internacional de Telecomunicaciones con sede en Ginebra. Este y sus filiales son los organismos que regulan las comunicaciones internacionales.

---

[117] Parlamento Europeo, Comisión Temporal Sobre el Sistema de Interceptación Echelon, La Secretaría, p.2

El artículo 37 del CIT establece lo siguiente:

"1. Los Miembros se comprometen a adoptar todas las medidas que permita el sistema de telecomunicación empleado para garantizar el secreto de la correspondencia internacional.

2. Sin embargo, se reservan el derecho a comunicar esta correspondencia a las autoridades competentes, con el fin de garantizar la aplicación de su legislación nacional o la ejecución de los convenios internacionales de que sean parte."[118]

La advertencia sobre el respeto del secreto de las telecomunicaciones se refiere sólo a la "legislación nacional" de los Estados. Los acuerdos SIGINT entre el Reino Unido, los Estados Unidos y otros países no constituyen "convenio internacional" alguno, lo cual es ventaja para ellos. En principio, el Convenio sólo autoriza que el cumplimiento de la ley se vea comprometido si el objetivo es garantizar la propia aplicación de la legislación.

El Convenio de Viena sobre relaciones diplomáticas (1961) afecta sólo a los gobiernos, pero es más específico; su artículo 27 establece lo siguiente:

"1. El Estado receptor permitirá y protegerá la libre comunicación de la misión para todos los fines oficiales. Para comunicarse con el Gobierno y con las demás misiones y Consulados del Estado acreditante, donde quiera que radiquen, la misión podrá emplear todos los medios de comunicación adecuados, entre ellos los correos diplomáticos y los mensajes en clave o en cifra. Sin embargo, únicamente con el consentimiento del Estado receptor podrá la misión instalar y utilizar una emisora de radio.

---

[118] Parlamento Europeo, Comisión Temporal Sobre el Sistema de Interceptación Echelon, La Secretaría, p.3

2. La correspondencia oficial de la misión es inviolable. Por correspondencia oficial se entiende toda correspondencia concerniente a la misión y a sus funciones."[119]

El artículo 30 establece que:

"1. La residencia particular del Agente diplomático goza de la misma inviolabilidad y protección que los locales de la misión.

2. Sus documentos, su correspondencia y, salvo lo previsto en el párrafo 3 del artículo 31, sus bienes, gozarán igualmente de inviolabilidad."[120]

Como se ha mencionado con anterioridad el campo de acción de Echelon no tiene fronteras, ya que los agentes diplomáticos no son ajenos a sufrir algún tipo de espionaje, y aunque existe ya un instrumento jurídico con carácter internacional que protege las actividades diplomáticas (en cuanto telecomunicaciones) parece de poco o nada servir en la actualidad.

3.6 La polémica

El espionaje internacional practicado por la red Echelon no tiene límites. Todo el mundo está dentro de su campo de acción, todo el mundo está potencialmente destinado a ser espiado. Se da el caso curioso de que la legislación de Estados Unidos prohíbe a la NSA el espionaje dentro de sus fronteras (que no en el resto del planeta), así que son los británicos los encargados de espiar a los Estados Unidos y luego se intercambian las informaciones entre agencias. Sin embargo, a raíz de los atentados contra los

[119] *Idem*
[120] *Idem*

Estados Unidos del 11 de septiembre del 2001 las leyes estadounidenses se están modificando para otorgar más poderes de espionaje interno a sus organismos de seguridad.

La verdadera polémica nace cuando se acusa a los gobiernos implicados en el espionaje a través de Echelon de haber extralimitado su campo de acción hacia el espionaje industrial y político en beneficio de los gobiernos implicados en la red. Es curioso que con anterioridad ningún gobierno recriminara la violación del derecho a la intimidad y privacidad del ciudadano común y corriente. Esto se explica porque se sobreentiende que todos los gobiernos practican ese tipo de espionaje, así que poco tienen que echar en cara a los demás. Además, no existe una legislación internacional que regule este tipo de acciones... y aunque existiera la situación no cambiaría considerablemente debido a que los gobiernos prefieren combatir problemas como el terrorismo, conflictos bélicos, narcotráfico, pornografía y/o prostitución infantil. Y no preocuparse por combatir la privacidad de aquella persona que solo utiliza el internet para ver su correo y bajar canciones.

El Parlamento Europeo creó la Comisión Echelon, como consecuencia del informe *Development of Surveillance Technology and Risk of Abuse of Economic Information*, publicado por el físico escocés Duncan Campbell:[121]

[121] Duncan Campbell fue la persona que investigó y reveló la existencia de Echelon.

DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

Vol 2/5

The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition

Working document for the STOA Panel

Luxembourg,October 1999 PE 168.184/Vol 2/5

fuente: Duncan Campbell, Development of Surveillance Technology and Risk of Abuse of Economic Information, p.1

Cataloguing data:

Title:	**Part 2/5:The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband ulti-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition**
Workplan Ref.:	EP/IV/B/STOA/98/1401
Publisher:	European Parliament Directorate General for Research Directorate A The STOA Programme
Author:	Duncan Campbell - IPTV Ltd.- Edinburgh
Editor:	Mr Dick HOLDSWORTH, Head of STOA Unit
Date:	October 1999
PE number:	**PE 168. 184 Vol 2/5**

fuente: Duncan Campbell, *Development of Surveillance Technology and Risk of Abuse of Economic Information, p.2*

El informe presentado por el periodista escocés fue presentado en 1999 y en él Campbell confirma la existencia de la red Echelon y su implicación en el espionaje a Gobiernos, organizaciones y empresas europeas. Es decir, que una

tecnología con origen militar se está utilizando con fines económicos y de espionaje industrial para favorecer a empresas pertenecientes a países integrantes de la red en detrimento de empresas mayormente europeas y japonesas. Estas empresas no son cualquier empresa. Son empresas, principalmente norteamericanas, relacionadas directamente con la red Echelon y con el sistema defensivo y militar de los Estados Unidos, como por ejemplo la firma aeronáutica McDonnell Douglas, o empresas punteras en campos tan críticos como telecomunicaciones, ingeniería genética o laboratorios de desarrollo de armas químicas y bacteriológicas. Esto se puede deber a que al gobierno de los EE.UU le interesa que esas empresas se mantengan fuertes, aunque la posibilidad más acertada sería que al estar esas empresas muy relacionadas con el Gobierno (por no decir que son una rama del mismo) sería ésta una forma más de controlar esos sectores tan importantes.

Se ha creado un gran revuelo e incluso Francia se plantea acusar formalmente a Gran Bretaña de traición a la Unión Europea, ya que sus acciones perjudican directa y conscientemente la economía de la Unión Europea en beneficio de un enemigo comercial directo, como son los Estados Unidos. Se habla también de que Gran Bretaña podría estar violando la Convención de Derechos Humanos de la UE respecto a la privacidad. Gran Bretaña se defendió alegando que sus leyes permiten espiar las comunicaciones para defender sus intereses económicos. Estados Unidos, fiel a su tradición, ha negado todo conocimiento y Nueva Zelanda mostró su preocupación ante una más que posible investigación por parte de la Unión Europea de su base de escuchas[122] en Waihopai, usada para el espionaje de la región del Pacífico, y aseguró que desde esas instalaciones no se realizan escuchas de "carácter comercial". Australia reconoció en 1999 la existencia de UKUSA y su pertenencia al mismo. El Gobierno español afirma la existencia de

[122] Base de espionaje.

la red y sostiene que intercepta millones de comunicaciones oficiales, comerciales y personales.

Actualmente se reconoce abiertamente la existencia de la red, si bien se niega que se utilice para realizar espionaje industrial y político, alegando que sus campos de acción son el terrorismo y las mafias.

3.7 Echelon Bajo la legislación europea

En cuanto a la protección contra el monitoreo por parte de las autoridades públicas, los estados europeos se rigen cada uno por su ley y constitución nacional[123] y por el *European Convention on Human Rights*. Esta última, tan amplia que su alcance incluye a internet, es particularmente interesante porque limita las medidas adoptadas por las leyes nacionales de los Estados firmantes para permitir el monitoreo de las comunicaciones en general, y de comunicaciones en internet en particular, por las autoridades gubernamentales, así como su poder para adoptar tales medidas.[124]

La sección 8 de este *Convenio*, que garantiza el derecho de privacidad y confidencialidad de la correspondencia, tiene consecuencias para las autoridades públicas. Por un lado, deben asegurar el respeto a la privacidad entre usuarios individuales; por el otro, deben abstenerse por sí mismas de toda interferencia, a menos que se satisfagan ciertas condiciones acumulativas. La excepción también debe estar prescrita por la ley[125]; la interferencia debe ser necesaria y proporcionada por las normas de una sociedad democrática y, por último, debe tener como objetivo la seguridad nacional, seguridad pública,

---

[123] El secreto de la correspondencia, que es muy similar a la protección de privacidad, está protegido bajo varias constituciones europeas.
[124] *cfr* Oliver Hance, *Leyes y negocios en Internet*. Traduc. Yazmín Parra. p. 121
[125] La noción de "prescrito por ley" comprende la legislación común en particular a los ojos de la Corte.

beneficio económico del país, orden público y prevención delictiva, protección de salud o moral y protección de los derechos y libertades de otras personas. Luego entonces, quedan estrictamente limitados los casos en los que la autoridad pública europea puede quebrantar los derechos de confidencialidad, discreción y de privacidad.

El 6 de septiembre de 1978, la Corte Europea de Derechos Humanos declaró que, aunque en la sección 8 del *Convenio* no se mencionan las conversaciones telefónicas, sí son parte integral de los conceptos de "privacidad" y "correspondencia"; en consecuencia, se benefician de esta misma protección. "Sobre la base de esta sección 8 y de la jurisprudencia de la Corte, los Estados miembros del Comité de Europa ahora están obligados a *adoptar regulaciones claras y precisas referentes a las situaciones en las que autoriza la intercepción telefónica o de comunicaciones electrónicas*".[126] En mi opinión, la confidencialidad de los varios tipos de comunicación interpersonal en internet (correo electrónico, Chat, video conferencia) también amerita, a todas luces, esta protección. Hacer circular un mensaje electrónicamente no altera el derecho de privacidad del emisor.

En aplicación de esta jurisprudencia europea, la legislación francesa 91-646 del 10 de julio de 1991, sobre la confidencialidad de correspondencia transmitida por telecomunicaciones,[127] estipula los casos en los que las autoridades públicas pueden grabar el contenido de la información transmitida, o rastrear el marcado de ciertos números telefónicos con un dispositivo específico, o al marcar desde una unidad específica. La ley limita esta violación de los derechos de confidencialidad a casos de necesidad justificada por cuestiones de interés público y prescritos por ella misma. La ley se aplica a dos tipos de intercepción: legal, sólo posible en el contexto de una petición legal y que solo se autoriza en caso de una ofensa lo suficientemente seria, y la

[126] Oliver Hance, *Leyes y negocios en Internet*. Traduc. Yazmín Parra p. 121
[127] O.J. de julio 1991

intercepción por razones de seguridad o administrativas, que deben fundamentarse en una de las bases legales de interceptación enumeradas en la sección 3 de la ley como lo es la prevención de terrorismo o de delitos, por ejemplo).

De manera similar, bajo la legislación inglesa, la Secretaría de Estado puede, con fundamento en el *Interception of Communications Act* de 1985, otorgar órdenes de intercepción por razones de seguridad nacional o por razones de prevención y detección de delitos en casos de delitos suficientemente graves, o para salvaguardar los intereses económicos del país.

Otro punto de partida es la sección 5 del Acta de Telegrafía Inalámbrica de 1949, la cual señala como ilegal el uso de cualquier aparato de telegrafía inalámbrica con el objetivo de obtener información, ya sean direcciones, contenidos de cualquier mensaje, el cual el usuario no esta autorizado a recibir o publicar la información obtenida de esa manera. Esta disposición no aplica a la intercepción autorizada por el gobierno y a la revelación de mensajes en procedimientos legales.[128]

La sección 2 del Acta de Intercepción de Comunicaciones de 1985, permite al Secretario de Estado autorizar la intercepción del sistema de telecomunicaciones, en caso de que sea necesario:

- sí atenta contra los intereses de la seguridad nacional,
- sí el propósito es para prevenir o detectar serios crímenes
- sí el propósito es salvaguardar el bienestar de la economía de Gran Bretaña.

Esta Acta proporciona un procedimiento para interceptar mensajes en internet, pero no mensajes siendo transmitidos dentro de redes privadas.

[128] *cfr* Dr Chris Elliott, *The legality of the interception of electronic communications*, p.8

Intercepciones de señales de teléfonos celulares esta excluido, (pero la subsiguiente transmisión de esas señales vía celular esta incluida ya que se le considera como una telecomunicación publica).

La Sección 1 del Acta de Mal uso de Computadoras de 1990 marca como un crimen ejecutar en una computadora una función con objeto de obtener acceso no autorizado de cualquier programa o información en cualquier otra computadora.

No existen restricciones legales en el Reino Unido sobre la importación, posesión o el uso de equipo encriptado. Sin embargo en caso de procedimientos legales, la Sección 20 del Acta de la Policía y Evidencia Criminal de 1984, permite a las autoridades consultar información de cualquier computadora.[129]

3.8 Echelon Bajo la legislación estadounidense

En Estados Unidos y Canadá, la protección a la privacidad o privacía en el sector público está garantizada por el derecho constitucional de privacía, que se aplica completamente a las comunicaciones electrónicas y, por lo tanto, a internet. Esta protección constitucional se aplica solamente a organismos gubernamentales o a la "acción del Estado". [130]

La interceptación de comunicaciones es generalmente ilegal en los Estados Unidos de América, pero es permitida en la mayoría de los Estados bajo severas reglas designadas a la protección de la privacidad, estas severas reglas

---

[129] *Ibidem* p.9.
[130] *cfr* Oliver Hance, *Leyes y negocios en Internet*. Traduc. Yazmín Parra. p. 119.

autorizan la investigación de un crimen gracias un requerimiento obtenido por una corte antes de dirigir la intercepción.

Existen dos básicas piezas en la legislación federal estadounidense: ECPA[131], la cual involucra investigaciones criminales y FISA[132], la cual involucra operaciones de inteligencia y contraespionaje.

Por virtud de las leyes o disposiciones de protección a la privacía (el *Electronic Communications Privacy Act ECPA*[133] en Estados Unidos y el *Criminal Code*[134] en Canadá), *la intercepción de comunicaciones electrónicas* por agencias de procuración de justicia requiere una búsqueda u otro tipo de autorización. De esta manera, la policía no puede interceptar el contenido del correo electrónico sin alguna orden. A pesar de esto, se debe hacer notar que la *ECPA* estadounidense faculta a autoridades de procuración de justicia a emplear dispositivos técnicos que puedan utilizarse para grabar números marcados desde un teléfono. La aplicación de estas medidas en internet probablemente liberaría a las autoridades de procuración de justicia estadounidenses de la necesidad de una orden de búsqueda para la identificación de computadoras que establezcan una conexión con una computadora bajo vigilancia.

ECPA trabaja como cualquier estructura institucional, establece un procedimiento que autoriza la intercepción legal. También vale la pena señalar que la *ECPA* prohíbe el *acceso, sin la orden de búsqueda, a la información almacenada en una computadora.*

Para obtener información en el extranjero, *FISA* esta autorizada para permitir vigilancia electrónica fuera de territorio estadounidense. *FISA* delimita su

[131] Electronic Communications Privacy Act 1986.
[132] Foreign Intelligence Surveillance Act 1978.
[133] *Electronic Communications Privacy Act* of 1986
[134] *Criminal Code* (Canadian), 1985

accionar en términos de la seguridad nacional, incluyendo defensa en contra de un ataque, sabotaje, terrorismo y actividades clandestinas de alguna inteligencia desconocida. Los objetivos no necesitan estar necesariamente relacionados con algún crimen. Las acciones de vigilancia de *FISA* son ejecutadas por el FBI. La vigilancia electrónica llevada por *FISA* es clasificada.[135]

FISA se divide en dos ramas:

- *"Comunicaciones a ó de personas norteamericanas, pero no norteamericanos que están en el extranjero. Una Corte autoriza la intercepción.*

- *Comunicaciones entre servicios de inteligencias internacionales. Esta intercepción puede ser autorizada por una orden Presidencial"*[136].

Por último, bajo la legislación estadounidense, ciertos servidores de internet profesionales quizá se beneficiarán de la protección adicional proporcionada por el *Privacy Protection Act*[137] de 1980.[138] El *Acta*, evidentemente, *protege a los editores electrónicos contra la búsqueda y confiscación de todo el "material relacionado con el cumplimiento de su trabajo"* en la posesión de una parte que difunda una forma de comunicación pública en el contexto o afectación del comercio interestatal.[139] A pesar de esto, esta protección contra confiscación no incluye casos donde existe una razón válida para creer que la persona en posesión de los datos ha cometido o está cometiendo un delito relacionado con

---

[135] *cfr* Dr Chris Elliott, *The legality of the interception of electronic communications*, p.10.
[136] *Ibidem* p. 12
[137] *Privacy Protection Act of 1980*, 42 U.S.C.s. 2000aa (1980).
[138] *cfr* Oliver Hance, *Leyes y negocios en Internet*. Traduc. Yazmín Parra, p. 120
[139] Materiales producto de trabajo puestos por una persona que se crea razonablemente que tenga el propósito de diseminarlo al público en un diario, libro, radiodifusión, u otro medio similar para su comunicación pública, para afectar el comercio interestatal. *Privacy Protection Act of 1980.*

este material o cuando existe confiscación inmediata es necesario prevenir que un ser humano sea seriamente afectado o incluso ser sujeto de homicidio.

CONCLUSIONES

CONCLUSIONES

Las nuevas tecnologías traen consigo avances favorables para una mejor vida pero también implican amenazas emergentes que pueden salirse de control, como por ejemplo: *la obtención de información y la elaboración de Inteligencia*, esenciales para la Seguridad Nacional, tanto en su componente civil como en el militar.

En las actuaciones policiales de los estados democráticos, las fuerzas de seguridad necesitan la autorización del juez para intervenir un teléfono. Pero en Echelon captan y graban todo lo que se les antoja. Echelon se convierte así en una amenaza para la libertad y el ejercicio de los derechos humanos en todo el mundo. Nadie está a salvo de que sus comunicaciones sean interceptadas, grabadas y archivadas. Nadie. Y las consecuencias de esa intromisión en nuestras comunicaciones quizás no podamos imaginarlas ahora, pero sí sabemos que la obsesión antiterrorista o antinarcotráfico como justificante de la utilización de Echelon nos hace ver la seguridad nacional como una doctrina paranoica. Y no se está contra Echelon porque no haya que luchar contra el terrorismo y cualquier otra actividad delictiva, claro que hay que luchar, pero los métodos como Echelon no son el camino; cuando en nombre de la máxima eficacia en cuestiones de seguridad se justifican los atropellos a los derechos humanos se está abriendo el camino al autoritarismo, a algún tipo de dictadura.

La red de espionaje internacional Echelon existe y desempeña perfectamente su trabajo sin encontrarse ningún obstáculo que frene su objetivo (ya sea técnico o legal), cuenta con una imponente infraestructura: presupuestos millonarios, tecnología de punta, apoyos gubernamentales, apoyos por parte de empresas líderes en su ramo y personal altamente especializado. Y si por alguna razón queda todavía algún recelo de su existencia, en junio del 2000 fue creada la Comisión Echelon con el objetivo de esclarecer las denuncias presentadas

ante el Parlamento Europeo sobre la existencia de una red de espionaje mundial capaz de entrometerse en los sistemas de comunicaciones europeos con gran facilidad, poniendo en riesgo estrategias políticas y económicas europeas, pero, sobre todo, vulnerando el derecho a la intimidad de los ciudadanos europeos y realizando prácticas comerciales desleales al entrometerse en las comunicaciones de la competencia. Incluso la Eurocámara recomienda a las empresas que se doten de los medios de protección necesarios para reducir su vulnerabilidad ante estos sistemas de espionaje; además de exhortar a los ciudadanos europeos a que codifiquen su correo electrónico

Es cierto que existen instrumentos jurídicos que protegen la privacidad de las comunicaciones como la Declaración Universal de Derechos Humanos, así como el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales y el Convenio Internacional de Telecomunicaciones, que garantizan la confidencialidad de ese tipo de comunicaciones; además que la lista de tratados burlados por las agencias sigint va en aumento, a los que el sistema Echelon parece desconocer su existencia, pero también es cierto que existen ciertas lagunas en estos instrumentos jurídicos que no protegen la privacidad en su totalidad ya sea en territorio o en alcance. Y es que en el pasado, absolutamente nadie que haya participado en la elaboración de algún instrumento jurídico que defiende la privacidad, habría imaginado el alcance que tendrían los avances tecnológicos en el futuro, por ejemplo, cuando se redactó la Constitución Americana era inconcebible que los soldados ingleses, derrotados y de vuelta en su patria, pudieran inmiscuirse en la intimidad de los hogares americanos. La situación ha cambiado, y con ella la cuestión de por qué el respeto de la intimidad de las telecomunicaciones debería circunscribirse a las fronteras nacionales. Es necesario reforzar la obligación de proteger la intimidad de las comunicaciones internacionales. Aunque la legislación nacional e internacional existente es, en principio, adecuada, es preciso consolidar las disposiciones vigentes con el fin de ampliar estos instrumentos y convenios, así como sus efectos. Si se establecieran nuevas disposiciones en materia de

colaboración internacional para la aplicación de la legislación, se reduciría el conflicto entre las actividades de SIGINT y los derechos humanos, ya que su ámbito se restringiría a objetivos específicamente militares y mucho más concretos en materia de seguridad nacional. Así pues el establecimiento de políticas en materia de protección de la privacidad, los criterios específicos de uso de información privada y la búsqueda del dialogo mediante cooperación internacional, son los principales retos a los que se debe hacer frente.

Lo cierto es que Echelon continúa realizando sus actividades de espionaje internacional a diario sin apego a un marco legal, sus actividades están violando los derechos de los ciudadanos así como el de los Estados, dañando la vida política, comercial, militar y económica de los Estados y ciudadanos espiados, así pues es necesario una urgente regulación a las telecomunicaciones en general como lo es el teléfono de uso domestico, teléfono celular, banda ancha, microondas, fax y por supuesto todo lo relacionado con el uso de computadoras como medio de comunicación ya sea correo electrónico y/o video conferencia e incluso aquellas emergentes.

Aunque la conciencia y la preocupación de la población van en aumento, no basta con estar alerta: si los países y los pueblos quieren integrarse en pie de igualdad en la infraestructura global de la información, es urgente aunar esfuerzos.

Por supuesto que las perspectivas que abre el escándalo Echelon son negras. Las nuevas tecnologías vienen a agregarse a nuestra sociedad (ya de por sí saturadas de estas). Echelon aparece como el método de control "perfecto": secreto, supuestamente infalible, libre de toda intromisión de la sociedad. Y sin embargo, es vulnerable. Los movimientos pacifistas han abierto varias brechas en contra de Echelon a través de "invasiones" a las bases del sistema y denunciando su existencia y sus actividades. Y algunas corrientes en pro de los derechos 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.

A lo largo de esta investigación he comprobado que prácticamente todas las notas periodísticas y páginas electrónicas especializadas que critican fuertemente el actuar de Echelon fueron elaboradas antes de los atentados del 11 de septiembre, incluso el día 5 de septiembre de 2001 el Pleno del Parlamento Europeo aprobó una resolución histórica donde denunciaba la existencia de una red de espionaje de las comunicaciones operada por Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda. Con lo anterior intento señalar que la comunidad internacional ya tenía conciencia de la existencia de esta red y ya se habían reunido elementos necesarios para iniciar una enérgica investigación en contra de Echelon. Pero después del 11- S, Estados Unidos y Gran Bretaña iniciaron la guerra contra el terrorismo, donde Echelon era y es un arma fundamental. Así la prioridad de atender la problemática de la violación de la privacidad en las comunicaciones fue dejada a un lado por el atender el terrorismo.

En un plano realista y severo Echelon tiene los suficientes elementos para seguir operando normalmente: oficialmente no existe, sus creadores y operadores minimizan o niegan su existencia, su accionar es secreto por lo cual es difícil darse cuenta sí un país, empresa o ciudadano esta siendo espiado, enterarse de que se esta siendo blanco de espionaje no es algo a lo que uno se enfrente todos los días y ¿como demostrarlo? ¿como obtener las pruebas? ¿dónde hacer la denuncia? Son cuestiones que todavía la sociedad no esta preparada para hacer frente. No hay manera de comprobar que se intercepten o no los mensajes de uno u otro país, ya que al tratarse de proyectos altamente clasificados, es imposible saber que es lo que se hace y pretende hacer. Esto debe cambiar con una legislación.

La hipótesis de este trabajo aseveraba que sí no se regulaba Echelon seguiría prevaleciendo su accionar y su intransigencia. Al analizar todos los elementos que predominan en el acontecer mundial actual, es indudable que esta hipótesis es comprobada. Echelon continuará llevando a cabo sus operaciones de espionaje militar, comercial, político y civil en todo el mundo, sin que exista algún tipo de instrumento jurídico internacional que enfrente tal situación evidenciando así la falta de atención a tal problema. Y aunque existiera una autoridad o un instrumento jurídico que limite o frene las actividades de Echelon, dudo mucho que Echelon acate esta autoridad y/o instrumento, solamente hay que recordar que Echelon realiza espionaje, realiza una actividad de carácter secreto, es decir, quizá algún día Echelon de fin a sus actividades pero, ¿como saber que eso es cierto?

Y es que el realismo como teoría política se construyó a base de entender la historia como el resultado de la naturaleza del ser humano a codiciar el poder y desear la dominación de otros. Siguiendo este supuesto, se determina que la posibilidad de erradicar el instinto por el poder es una aspiración utópica. Esto lleva a percibir la política internacional como una lucha interminable entre aquellos actores que intentan dominar a otros y aquellos que intentan resistir este dominio externo. El realismo político asume que el sistema internacional es anárquico, en el sentido de que no existe una autoridad superior a los estados capaz de regular efectivamente las relaciones entre ellos.

Tampoco parece acertado llegar a imaginar el siguiente escenario: una comitiva representante de la ONU inspeccionando las bases de Echelon, acordonando la zona y poniendo un sello de "clausurado" y después poner en subasta todo el equipo recaudado. Imposible, seguramente Echelon lo sabría con anterioridad y tomaría las medidas necesarias. Suponiendo que esto pueda ser posible (siendo muy optimista) quien dice que no se pueda desarrollar otras formas para llevar a cabo el espionaje internacional, al fin y al cabo sabemos

que la tecnología avanza tan rápido que cada día el hombre encuentra nuevas formas de aprovecharlas para su conveniencia.

ANEXOS

ANEXO 1

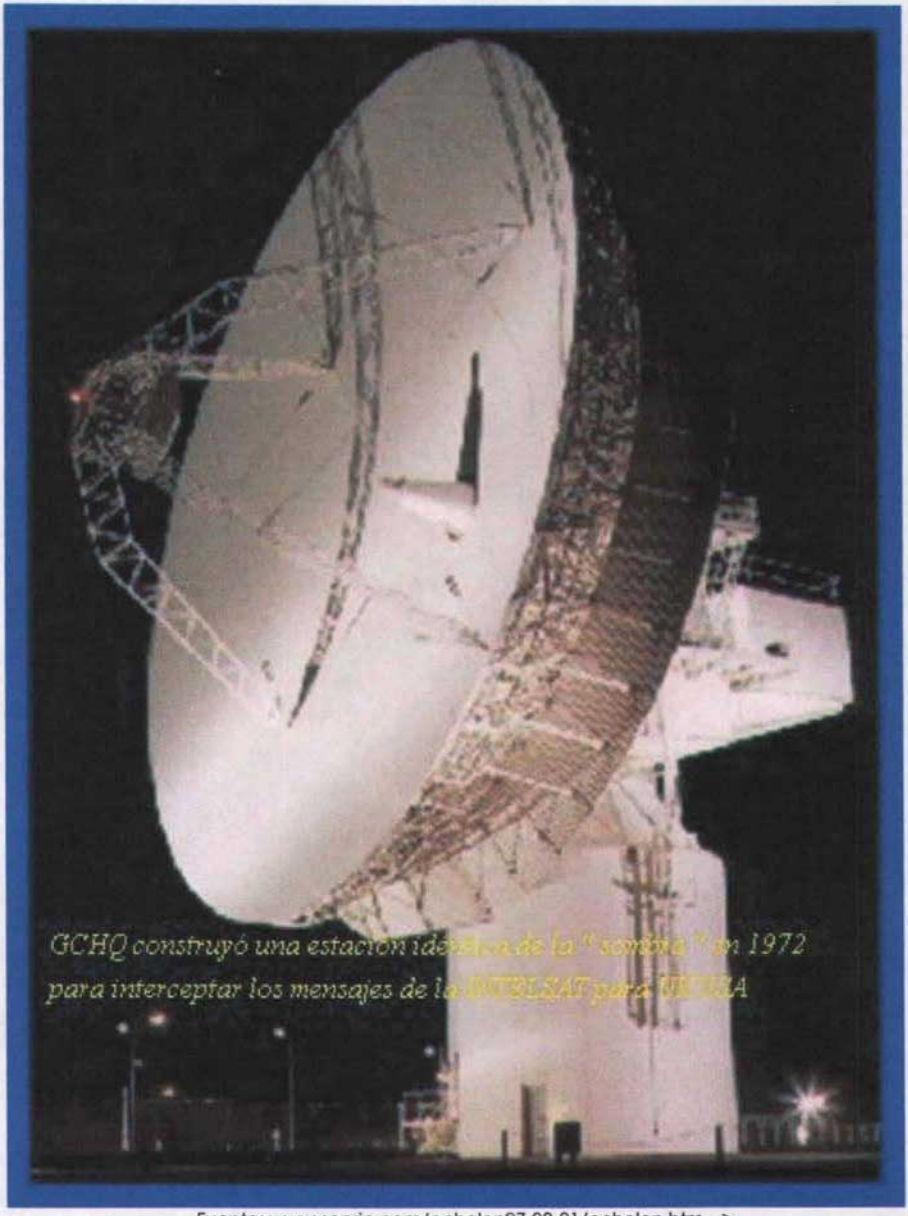
FOTOS DE LAS BASES DE ECHELON

Fuente: www.seprin.com/echelon27-08-01/echelon.htm -->

Fuente: www.seprin.com/echelon27-08-01/echelon.htm -->

Fuente: www.seprin.com/echelon27-08-01/echelon.htm -->

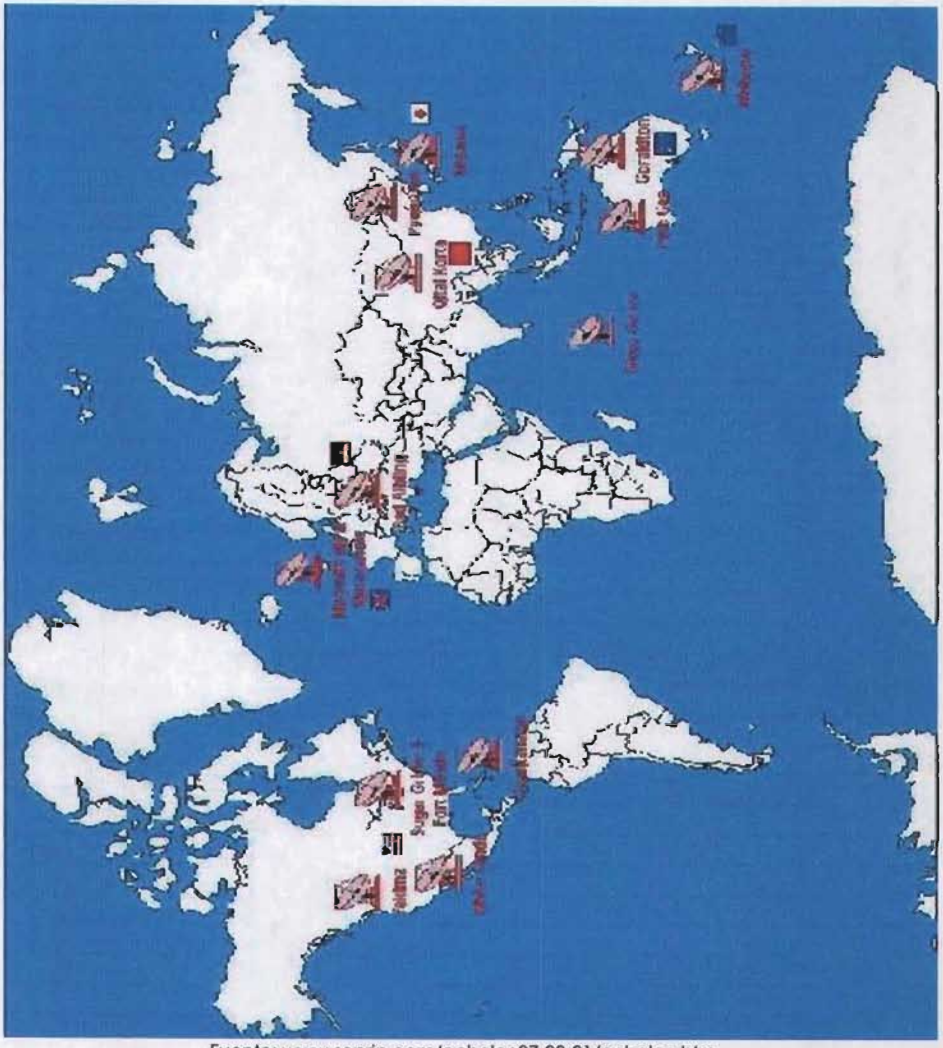
Fuente: www.seprin.com/echelon27-08-01/echelon.htm -->



Fuente: www.seprin.com/echelon27-08-01/echelon.htm -->

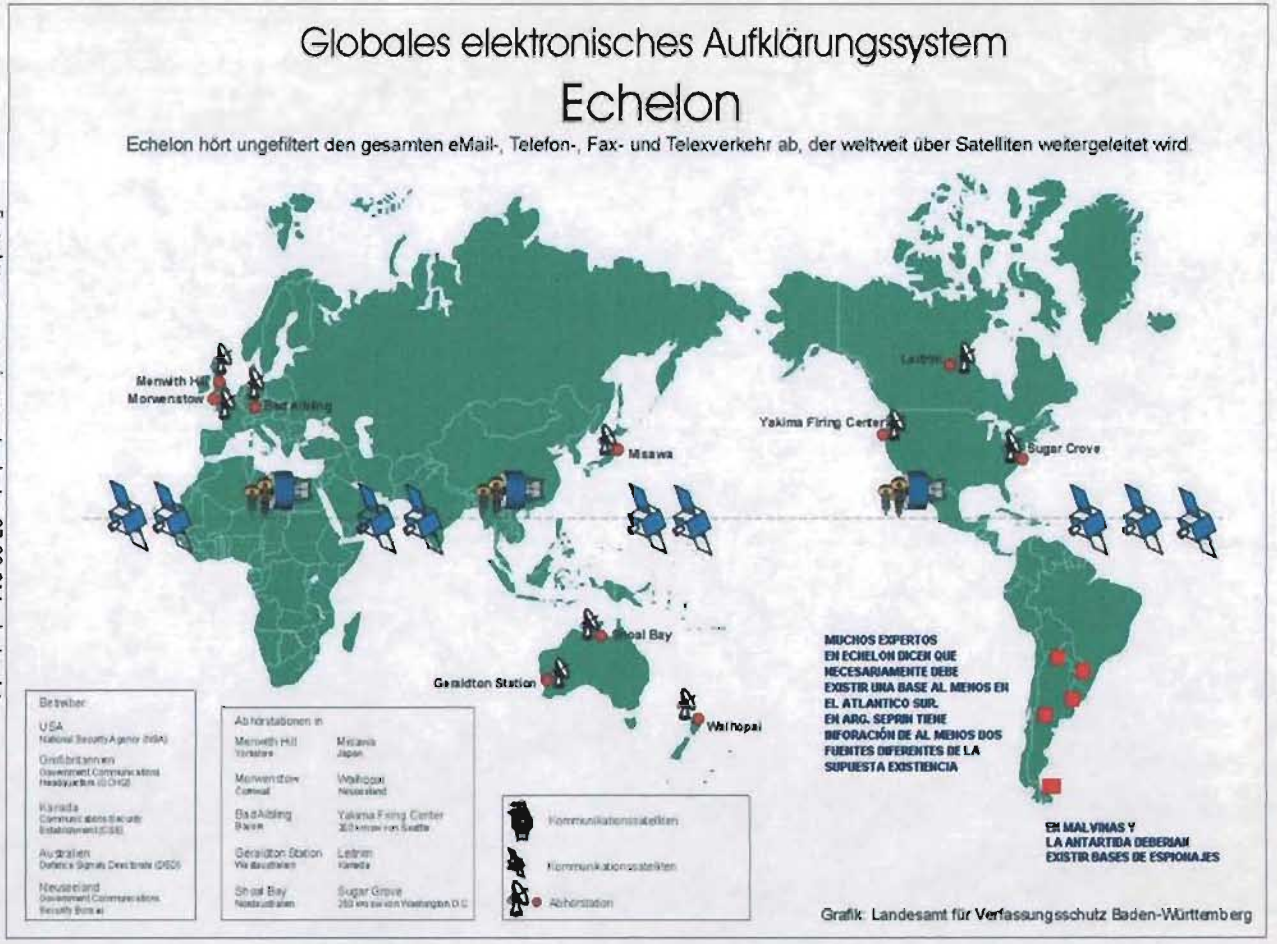
Anexo 2

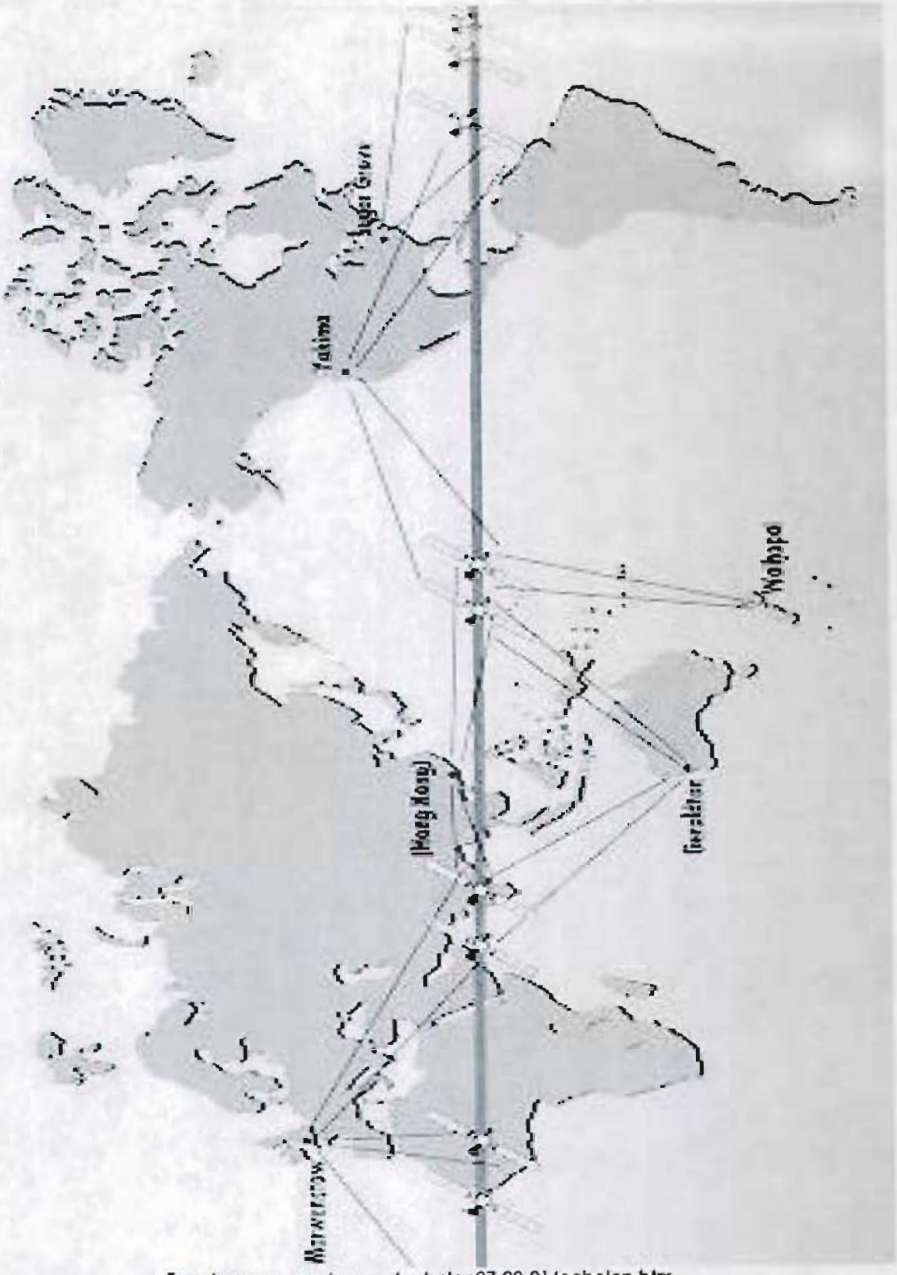
MAPAS DE DISTRUBUCIÓN Y ESTACIONES TERRENAS DE ECHELON



Fuente: www.seprin.com/echelon27-08-01/echelon.htm

Fuente: www.seprin.com/echelon27-08-01/echelon.htm





Fuente: www.seprin.com/echelon27-08-01/echelon.htm

Anexo 3

INFORME DESCLASIFICADO DE LA NSA SOBRE LA EXISTENCIA DE ECHELON

COPY

UNCLASSIFIED

NSCID 9
ised
O, 1950

NATIONAL SECURITY COUNCIL INTELLIGENCE DIRECTIVE NO. 9

COMMUNICATIONS INTELLIGENCE

Pursuant to the provisions of Section 101 and Section 202 of the National Security Act of 1947, as amended, the National Security Council hereby authorizes and directs that:

1. There is hereby established under the National Security Council the United States Communications Intelligence Board (hereinafter referred to as the "Board") to effect the authoritative coordination of Communications Intelligence activities of the Government and to advise the Director of Central Intelligence in those matters in the field of Communications Intelligence for which he is responsible.

2. The Board will be composed of not to exceed two members from each of the following departments or agencies: The Departments of State, the Army, the Navy, and the Air Force, and the Central Intelligence Agency, and the Federal Bureau of Investigation. Only those departments or agencies designated by the President are authorized to engage in Communications Intelligence activities.

3. The Board members will be vested with authority to represent their respective departments or agencies in the field of Communications Intelligence and each member department or agency will be represented at each meeting by at least one member, or alternate, with the necessary powers to act.

4. Decisions of the Board will be based on the principle of unanimity, which shall be a prerequisite for matters within the purview of the Board, except that the Chairman shall be elected by majority vote. When decision cannot be reached, the Board will promptly refer the matter for resolution to the National Security Council; provided that, when unanimity is not obtained among the military department heads of the Department of Defense, the Board shall present the problem to the Secretary of Defense before presenting it to the National Security Council.

5. Decisions and policies promulgated by the Board within the scope of its jurisdiction shall be applicable to all departments and agencies represented on or subordinate to the National Security Council and any others designated by the President, and shall be implemented by those departments and agencies of which action is required.

- 1 -

1 pan 49

NSCID 9
Revised
March 10, 1950

[redacted] Sec 3.3(b)(6)
By the National Security Council
under provisions of E.O. 12958
by [redacted]

UNCLASSIFIED

Fuente: www.seprin.com/echelon27-08-01/echelon.htm

6. The special nature of Communications Intelligence activities requires that they be treated in all respects as being outside the framework of other or general intelligence activities. Orders, directives, policies, or recommendations of any authority of the Executive Branch relating to the collection, production, security, handling, dissemination, or utilization of intelligence, and/or classified material, shall not be applicable to Communications Intelligence activities, unless specifically so stated and issued by competent departmental or agency authority represented on the Board.

7. The Board shall act for the National Security Council to insure proper and full implementation of Council directives by issuing such supplementary directives as may be required. Such implementing directives in which the Board concurs unanimously shall be issued to and implemented by the member departments and agencies. When disagreement arises in the Board upon such directive, the proposed directive, together with statement of non-concurrence, shall be forwarded to the National Security Council decision as provided in paragraph 4.

8. Other National Security Council Intelligence Directives to the Director of Central Intelligence and related implementing directives issued by the Director of Central Intelligence shall be construed as non-applicable to Communications Intelligence activities under the authority of paragraph 6 above, unless the National Security Council has made its directive specifically applicable to Communications Intelligence.

9. The Board will perform such functions as may be required to accomplish its objective set forth in paragraph 1 above, and in the exercise of responsibilities and authority delegated to it by the National Security Council in this directive.

10. The Board shall leave the internal administration and operation of Communications Intelligence activities to the member departments or agencies.

11. All currently effective decisions, policies, and operating arrangements of the Board and its predecessors, the Army-Navy Communications Intelligence Board, and the State-Army-Navy Communications Intelligence Board, as previously constituted, which are not in conflict with this directive, will remain in full force and effect unless changed by subsequent decisions of the Board.

12. Definitions. For purposes of this directive the following definitions apply:

a. "Foreign communications" include all telecommunications and related materials (except Foreign Press and Propaganda Broadcasts) of the government

9
ed
10, 1950

and/or their nationals or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor; they shall include all other telecommunications and related material of, to, and from a foreign country which may contain information of military, political, scientific or economic value.

b. "Communications Intelligence" is intelligence produced by the study of foreign communications. Intelligence based in whole or in part on Communications Intelligence sources shall be considered Communications Intelligence as pertains to the authority and responsibility of the United States Communications Intelligence Board.

c. "Communications Intelligence Activities" comprise all processes involved in the collection, for intelligence purposes, of foreign communications, the production of information from such communications, the dissemination of that information, and the control of the protection of that information and the security of its sources.

CID 9
ded
h 10, 1950

Anexo 4

ENTREVISTA NO. 1
ENTREVISTA CON DUNCAN CAMPBELL

"Espían todas las comunicaciones de la Argentina"

Entrevista con Duncan Campbell

El periodista e historiador escocés que denunció ante el Parlamento Europeo la red de espionaje satelital Echelon asegura que hay cuatro bases que controlan a nuestro país (Argentina).

Como opera el sistema

El sistema Echelon es una inmensa red de espionaje que, utilizando más de 120 satélites y gigantescas redes de computadoras, intercepta millones de llamadas telefónicas, e-mails y faxes en todo el mundo.
Este sistema fue desarrollado con propósitos defensivos a principios de la década del 70, en plena Guerra Fría, por los servicios de inteligencia estadounidense, británico, canadiense, australiano y neozelandés.
Después de la caída del Muro de Berlín y del colapso de la Unión Soviética, Echelon comenzó a ser utilizado para el espionaje industrial.
¿Cómo opera Echelon? Los satélites espías recolectan una inmensa cantidad de mensajes y las remiten a las antenas parabólicas que, a su vez, las reenvían a computadoras que buscan en los mensajes palabras clave. Los despachos seleccionados son sometidos a un nuevo proceso de selección en las agencias de espionaje para detectar datos de interés.

Nuevos elementos se suman al escándalo internacional desatado por las denuncias sobre Echelon, una red de vigilancia global de las telecomunicaciones en la que se involucra a los servicios de inteligencia de los Estados Unidos, Gran Bretaña; Canadá, Australia y Nueva Zelanda.
Desde estos dos últimos países se interceptaron las comunicaciones argentinas durante la guerra de Malvinas, según las declaraciones que hace ahora a Clarín el hombre que el miércoles dio al Parlamento Europeo las evidencias más contundentes sobre las actividades de Echelon.

Las comunicaciones latinoamericanas son sistemáticamente monitoreadas desde cuatro bases de intercepción, y también Europa nos espía, revela en esta entrevista exclusiva el escocés Duncan Campbell, periodista de investigación, consultor del Parlamento Europeo en materia de inteligencia y comunicaciones y actualmente el más renombrado experto en política electrónica.

-Usted dijo que la NSA National Security Agency tendría acceso a toda la información confidencial de México. ¿Qué pasa con la Argentina?

-Buena parte de las comunicaciones mexicanas pasan a los Estados Unidos de manera directa, de modo que no hace falta ninguna estación especial para interceptarlas. Ese no es el caso de la Argentina. Las comunicaciones argentinas o latinoamericanas son interceptadas y monitoreadas sobre todo cuando se realizan vía satélite. Con ese propósito, los Estados Unidos, Canadá y Gran Bretaña tienen bases de intercepción satelital que pueden recibir esas comunicaciones y procesarlas en el sistema Echelon.

-Se habla de que hay dos bases que interceptan las comunicaciones del sur de América. ¿Es verdad?

Son cuatro bases: Puerto Rico, Canadá (cerca de Ottawa), Estados Unidos (cerca de Washington) y la cuarta está en el sur de Inglaterra.

-También se dice que la red Echelon espió a la Argentina durante la Guerra del Atlántico sur. ¿Qué sabe usted al respecto?

-Había bases en Australia y Nueva Zelanda que se utilizaron para monitorear las comunicaciones argentinas y transmitirlas a estaciones de escucha británicas. Me parece un asunto verdaderamente lamentable, algo muy estúpido. A decir verdad, sin embargo, a ningún país que esté en guerra debería sorprenderle que se espíen sus comunicaciones. Sí, por supuesto: Gran Bretaña y sus aliados lo hicieron. Creo que es más importante destacar el hecho de que los países que no se encuentran en guerra -como es ahora el caso de Gran Bretaña y Argentina- continúen espiando o siendo espiados.

-Se habla de un sitio de colección de comunicaciones satelitales en Kourou, Guyaña, que espía a Sudamérica. Usted no lo menciona entre las bases de Echelon.

-Hay una base sobre la que informaron periodistas franceses y estaría ubicada en Kourou. Creo que su objetivo principal es América del Norte. Si esa base existe está dirigida por los franceses y su principal objetivo son los Estados Unidos. De todos modos, como estaría ubicada en Guyana, tiene posibilidades de monitorear también las comunicaciones

sudamericanas. Yo creo que es probable que las comunicaciones brasileñas y argentinas sean interceptadas por franceses y alemanes, pero no lo sé con certeza. De todos modos, esa base no forma parte de Eehelon. Pertenece a Francia y Alemania.

-Usted dijo que Microsoft colaboró con Echelon. Microsoft lo niega. ¿Usted lo sigue sosteniendo?

-¡No pueden negarlo! El browser (navegador de Internet) de Microsoft fue modificado en la versión que se distribuye al exterior. Y eso no es ningún secreto: si usted no es ciudadano de los Estados Unidos, es posible vulnerar la seguridad de su browser. Y eso fue lo que se hizo en los sistemas de la NSA, de modo que Microsoft no puede negarlo. Prácticamente lo admitieron. Dijeron que se había hecho para cumplir con las regulaciones de exportación de los Estados Unidos, y éstas exigen que, si algo sale de los Estados Unidos, la NSA pueda escucharlo.

-El informe presentado al Parlamento Europeo acusa también a IBM

-En lo que respecta al Lotus Notes (el programa de correo electrónico de IBM), la criptografía (N. de la R.: las normas para codificar comunicaciones y asegurar su privacidad) del sistema se hizo más débil cuando se lo vendió al exterior, o sea a compradores no estadounidenses.

-¿Hubo alguna respuesta?

-Lotus, que es la subsidiaria de IBM involucrada, hizo una serie de declaraciones. Básicamente, lo que dijeron fue que nunca lo habían ocultado. Y yo respondo: "Yo no digo que fuera un secreto, lo que digo es que esto se hizo". La posición de IBM es que ellos no hicieron un secreto de esto. El hecho es que cuando se convirtió en un tema polémico, la documentación se retiró de la librería y de Internet. De modo que sí lo mantuvieron un poco en secreto. Sin embargo, a mí no me interesa si era un secreto chico o grande. El punto es que lo hicieron.

-¿Cómo se explica que, después de todo lo informado al Parlamento Europeo, Echelon continúe actuando sin problemas?

-Se explica por el hecho de que las organizaciones de inteligencia involucradas son extremadamente poderosas, extremadamente bien establecidas, y han persuadido a los líderes políticos de que tener la posibilidad de espiar a otros políticos es algo que vale la pena.

-Pero Europa tiene información sobre Echelon desde hace al menos dos años. ¿No le parece que la reacción europea es lenta y no lo suficientemente enérgica?

-A decir verdad, yo denuncié el sistema Echelon por primera vez hace doce años, en 1988. En aquel momento, los medios no le prestaron ninguna atención. Seis años después se publicó el libro en Nueva Zelanda ("Secret Power: New Zealand's Role in the International Spy Network", de Nicky Hager) y la gente empezó a prestarle cada vez más atención. A los políticos y a los gobiernos les llevó mucho tiempo comprender qué es lo que en realidad está pasando.

-Según información reciente, el papa Juan Pablo II fue otro de los objetivos de Echelon. ¿Qué sabe de esto y cuál es su opinión?

-En la década del ochenta, la posición de la Iglesia Católica Romana en Europa y en todo el mundo sobre el desarme nuclear y las negociaciones de paz era un factor muy importante para la opinión pública mundial. La inteligencia británica y estadounidense querían estar al tanto de las conversaciones que mantenían entre sí el Papa y los cardenales sobre estos temas.

-Entonces no sólo estamos hablando de espionaje industrial.

-No, es político.

-Pero hasta ahora sólo se hablaba de espionaje industrial.

-Yo no. Se espía con fines militares, con fines políticos, con fines económicos.

CLARIN - lunes 6 de marzo de 2000

Fuente: http://www.buenosaires-links.com.ar/memo/recortes/echelon4.htm -->

ENTREVISTA NO. 2
ENTREVISTA CON MARGARET NEWSHAM

"Echelon fue como mi hijo"

Entrevista con Margaret Newsham Ex-Agente de la NSA en Echelon

Ekstra Bladet se encuentra con la espía de Echelon. A pesar de su enfermedad y la ansiedad que padece, nos revela como se llevó adelante el espionaje político.

Por Bo Elkjær y Kenan Seeberg.

LAS VEGAS (Ekstra Bladet): "A pesar de que me sentía mal acerca de lo que estábamos haciendo, estaba muy satisfecha con la parte profesional de mi trabajo. No quiero fanfarronear, pero era muy buena en lo que hacía, y me sentía como si Echelon fuera mi hijo."

Ekstra Bladet se encuentra con Margaret Newsham en su casa en un suburbio de Las Vegas. Por razones obvias, omitimos el nombre del lugar donde Margaret Newsham está intentando llevar una vida normal. Nunca ha mencionado su pasado a sus vecinos.

Un pasado en el que Margaret Newsham ha estado en contacto cercano con el núcleo del más secreto de este mundo. Margaret Newsham ayudó a construir el sistema de espionaje electrónico conocido como Echelon.

Hoy, ha roto toda conexión con el mundo del espionaje y vive con el miedo constante de que "ciertos elementos" de la NSA o la CIA intenten callar su voz. Como resultado, duerme con una pistola cargada bajo su colchón, y su mejor amigo es Mr. Gunther - un enorme pastor alemán que fue entrenado como perro guardián por un buen amigo de la Policía Estatal de Nevada.

Envió al perro a una "niñera" antes de que llegásemos, dado que "no deja entrar extraños en mi casa", dice con una débil sonrisa.

Antes, Newsham sólo había hablado una vez acerca de su trabajo como espía en Echelon: en audiencias de alto secreto realizadas por el Congreso de EEUU en 1988. Hoy,

Margaret rompe once años de silencio hablando a la prensa por primera vez acerca de su trabajo para la mayor red de espionaje de todo el mundo. Margaret Newsham decidió hablar con *Ekstra Bladet* a pesar de que su doctor le recomendó no hacerlo. "Tengo la tensión alta, mi doctor dice que corro un riesgo hablando con usted, pero es un riesgo que quiero tomar".

SENTENCIA DE MUERTE

La vida de Newsham ha sido un infierno desde que fue despedida de su trabajo en Lockheed Martin donde diseñaba programas para la red global de obtención de datos de Echelon. Cuando se le ofreció trabajar en un proyecto en 1984, se negó porque pensó que podría dañar al gobierno americano. Poco después, la gente de Echelon en la NSA (National Security Agency) se aseguró de que fuera despedida por Lockheed Martin. Inmediatamente después, denunció a su empleador por despido ilegal y contactó con la comisión de seguridad interna, DCAA, que llevó a cabo las audiencias privadas.

"Desde entonces me he sentido bajo mucha presión, lo que ha tenido una influencia fatal en mi salud," dice Margaret Newsham, quien ha sobrevivido a un ataque de apoplegía que la dejó totalmente paralizada. Todo lo que le quedaba era su sentido del oído cuando llegó al hospital.

"Podía escuchar al doctor pronunciando mi sentencia de muerte, mientras que mi marido y tres hijos se encontraban a mi lado. Lo único que me hizo seguir adelante fue pensar que, si moría, perdería mi caso. Ese pensamiento es lo que me devolvió a la vida."

Después de recuperar su movilidad, Newsham sufrió un paro cardíaco, y hace dos años tuvo que ser intervenida de un tumor maligno. Hoy, dice secamente que vive en tiempo "prestado", lo que quizá explica porque esta vez elige dar la cara.

ESPIANDO A LOS POLITICOS

"Para mí, sólo hay dos formas de ver las cosas: correcto o erróneo. Y cuanto más pasaba el tiempo trabajando en proyectos clandestinos de vigilancia, más me daba cuenta de que no eran ya ilegales, sino también inconstitucionales."

Margaret Newsham no está contenta consigo misma por participar en el espionaje de gente ordinaria, políticos, grupos de interés y compañías privadas, que es exactamente lo que hizo durante 10 años, desde 1974 a 1984. Tanto los satélites y los programas informáticos fueron desarrollados en el cuartel general de Lockheed en Sunnyvale, California, y en 1977, fue destinada al mayor puesto de escucha del mundo en Menwith Hill, Inglaterra.

"El día en Menwith Hill cuando me di cuenta de verdad de lo absolutamente equivocada que estaba, me encontraba sentada con uno de los muchos "traductores". Era un experto en lenguajes como ruso, chino y japonés. De repente me preguntó si quería escuchar una conversación que tenía lugar en EEUU en una oficina del Edificio del Senado. Entonces escuché claramente un dialecto sudamericano que pensé que había oído antes."

"¿Quién es ese? " pregunté al traductor, que me dijo que era el senador republicano Strom Thurmond. '¡ Oh, cielos !' pensé. No sólo estamos espiando en otros países, sino también a nuestros propios ciudadanos. Fue entonces cuando realmente me di cuenta de que lo que estábamos haciendo no tenía nada que ver con los intereses de seguridad nacional de EEUU."

EL CONOCIMIENTO ES PODER

En toda su compleja simplicidad, la agencia de inteligencia americana, NSA, junto con agencias de inteligencia en Inglaterra, Canadá, Australia y Nueva Zelanda, ha establecido un sistema de satélites y sistemas informáticos que pueden monitorizar todas las comunicaciones electrónicas a lo largo del mundo: conversaciones telefónicas, e-mails, telex y telefax. Otros cuantos países están afiliados como participantes de tercera o cuarta categoría, incluyendo Dinamarca.

El concepto fundamental del sistema es obtener acceso a todos los movimientos políticos importantes en países tanto hostiles como aliados y vigilar todos los movimientos económicos importantes. El conocimiento es poder, y la NSA lo sabe. Es más, los espías de la NSA sirven como la única autoridad para supervisar quién recibe la información y para qué es utilizada.

"Incluso entonces, Echelon era muy grande y sofisticada. Tan pronto como era 1979, podíamos seguir a una persona determinada y enfocar su conversación telefónica mientras se comunicaba. Desde que nuestros satélites en 1984 pudieron filmar un sello

de correos en el suelo, es prácticamente imposible imaginar la complejidad que el sistema debe poseer hoy en día.

ECHELON FUE UNA IDEA DE LA NSA

¿Quién estableció el nombre de Echelon?

"La NSA. El código alfanumérico de Lockheed Martin era P415."

¿Qué hiciste exactamente?

"Desafortunadamente, no puedo hablarte de todas mis tareas. Todavía estoy atada por el secreto profesional, y odiaría ir a prisión o verme en vuelta en cualquier problema, si sabes lo que te quiero decir. En general, puedo decirte que era responsable del compilado de varios sistemas y programas, configurando todo el sistema y haciéndolo operacional en mainframes [grandes computadores]

¿Qué parte del sistema es llamado Echelon?

"La red de ordenadores en sí. Los programas de software se conocen como SILKWORTH y SIRE, y uno de los satélites más importantes de vigilancia se llama VORTEX. Intercepta cosas como conversaciones telefónicas.

APROBADO POR LA CIA

¿Trabajaste como agente para la NSA, pero fuiste empleada por una compañía privada?

"Sí, es casi imposible describir la diferencia entre los agentes de la NSA y civiles empleados por Lockheed Martin, Ford e IBM. Las fronteras son muy difusas. Tuve una de las mayores clasificaciones de seguridad, que requerían la aprobación de la CIA, la NSA, la Armada y la Fuerza Aérea. Esta aprobación incluía tanto un test con detector de mentiras, como un test expandido de historia personal en el que mi familia y relaciones fueron comprobados discretamente por la agencia de seguridad."

El cielo se oscurece sobre las cascadas de neón de Las Vegas cuando Margaret Newsham nos habla de incontables infracciones de las regulaciones de seguridad y acerca de una de sus compañeras que sufrió daños cerebrales cuando participó en el desarrollo del bombardero Stealth. Aunque Margaret Newsham está totalmente agotada, también parece aliviada.

"Esta es la primera vez que he contado algunas de las cosas que te he dicho hoy. Pero quiero ir a recoger a Mr. Gunther pronto para sentirme segura de nuevo. Mide su presión arterial y parece muy alarmada.

"Será mejor que vaya a ver al doctor mañana por la mañana así que quizá podríamos encontrarnos de nuevo más tarde."

Cuando vuelve con Mr. Gunther una hora después, el perro inspecciona cada habitación antes de que Margaret entre. La última cosa que hace antes de caer dormida en su enorme cama, es comprobar su pistola para asegurarse de que sigue cargada.

Hechos:

Lockheed Martin es el mayor suministrador de municiones a los servicios militares de EEUU y a sus agencias de inteligencia, la NSA y la CIA. En los años 80, Lockheed Martin absorbió LORAL Space Systems y Ford Aeroespacial, quienes también proporcionan equipamiento de monitoriación a las agencias de espionaje. Margaret Newsham trabajó para la NSA a través de su empleo en Ford y Lockheed desde 1974 hasta 1984. En 1977 y 1978, Newsham fue destinada al mayor puesto de escucha del mundo en Menwith Hill, Inglaterra. Recibió entrenamiento sobre su trabajo en el cuartel general de la NSA en fort George Meade en Maryland, EEUU.

Ekstra Bladet posee las órdenes de Margaret Newsham, de destino del Departamento de Defensa de EEUU. Ella poseía la clasificación de alta seguridad TOP SECRET CRYPTO.

Según la información encontrada por *Elkstra Bladet* en las bases de datos del Pentágono, la NSA tenía 38,613 empleados en 1995. Esta cifra no incluye la gran cantidad de empleados de compañías privadas que trabajan para la NSA.

Ekstra Bladet ha documentado la existencia de Echelon en una larga serie de artículos en los últimos meses.

Dinamarca está afiliada como tercero a Echelon, y el puesto danés más importante de escucha está situado en Aflandshage en la isla de Amager.

VENDI MI VIDA AL GRAN HERMANO

"Los ministros de Dinamarca pueden creer en lo que quieran. Sé que Echelon existe, porque ayudé a crear el sistema." Por segundo día consecutivo, la espía de Echelon Margaret Newsham habla acerca de la parte oscura del espionaje - y de las fatales consecuencias que ha tenido en su vida. La mitad de sus antiguos compañeros están hoy muertos.

"Las inspecciones estaban increíblemente orientadas a objetivos concretos. Eramos capaces de aislar a un individuo o a una organización y monitarizar todas sus comunicaciones electrónicas - en tiempo real - y todo el tiempo. La persona era monitorizada sin siquiera tener una oportunidad de saberlo, y la mayor parte de la información era enviada a la velocidad de la luz a otra estación utilizando la enorme capacidad digital a nuestro servicio. Todo tenía lugar sin ninguna "garantía legal" en la búsqueda.

¿Era toda la información enviada al cuartel general de la NSA en Fort George Meade en Maryland?

"No toda, pero sí gran parte."

¿Utiliza el sistema programas capaces de registrar virtualmente las ondas en el aire basándose en ciertas categorías y palabras clave?

"Esa es una de las formas en que funciona, sí. Es como un buscador de Internet. Restringiendo tu búsqueda a determinados números, personas o términos, obtienes resultados que tienen que ver con aquello que quieras escribas lo que escribas.".

BRECHA DE SEGURIDAD

Ekstra Bladet se encuentra con Margaret Newsham en su casa en las afueras de Las Vegas. Hablando con *Ekstra Bladet*, elige romper su silencio y contarnos todo lo que considera razonablemente seguro para ella contar, dado que Newsham todavía está sometida a la *omertá* de los servicios de inteligencia. Según este código de silencio, no se le permite revelar nada acerca de sus actividades de espionaje para la NSA.

"Pero es difícil para mí vivir con el hecho de que vendí mi vida y mi libertad de expresión al mayor servicio de inteligencia del gobierno de EEUU." En general, es difícil para Margaret Newsham llevar una vida normal, aunque eso es lo que ella quiere hacer

por encima de todo. En 1984, fue despedica por Lockheed Martin, que construía equipamiento de espionaje para la NSA. Finalmente, se negó a trabajar en un proyecto que pensó que era un riesgo de seguridad. Fue "retirada" como ellos lo llaman - y ella les denunció por despido improcedente.

ESTAFADORES DEL BILLON DE DOLARES

"Experimenté brechas de seguridad casi cada día tanto en el cuartel general de Lockheed en Sunnyvale, California, y en Menwith Hill, Inglaterra. A veces era completamente absurdo. En la barbacoa de unos amigos del departamento responsable del desarrollo del bombardero Stealth, la tetera de la barbacoa estaba hecha del mismo material que hacía al bombardero invisible a los sistemas de radar hostiles. En otra ocasión, alguien tenía tazas de café y todas ellas estaban cubiertas con impresiones de estaciones altamente clasificadas de Echelon. Pero también estaban mezclados en estafas. Lockheed Martin vendió más barato que otras compañías para conseguir contratos de proyectos de la NSA, tras lo que ilegalmente transferían dinero y mano de obra para llegar al contrato. Dado que podían estafar a otros por millones de dólares, eran capaces de todo. Eso los hizo muy falsos, y a mis ojos, pusieron en peligro la seguridad del Gobierno de Estados Unidos."

¿Fue informado el Gobierno de Estados Unidos acerca de los proyectos clandestinos?

"No. Por eso los llamábamos "Programas Negros". El gobierno nunca supo realmente que estaba sucediendo para qué se estaban utilizando tantos billones. Y me sentía muy leal tanto al gobierno como a la Constitución Americana, que estaba siendo infringida constantemente. El mundo del espionaje también se llamó "El Mundo Negro" porque la mayoría de nuestras operaciones fueron llevadas en secreto, más allá de todo control."

Desde su despido, Margaret Newsham ha estado bajo fuertes presiones, dado que su caso contra Lockheed Martin podría significar que una corte arrojara luz sobre los "Proyectos Negros" de la NSA. Entre otras cosas, el caso tiene que ver con la estafa de más de 1.4 billones de dólares.

MUERTES PREMATURAS

El caso ha tenido un efecto fatal en su salud. Desde el 84 ha tenido un ataque que la dejó paralizada, sobrevivió a un ataque al corazón, y por encima de todo estuvo sufrir cáncer. Hoy, vive en "tiempo prestado", y sufre de alta tensión sanguínea.

"Tampoco ayudó en nada cuando mi marido me pidió el divorcio tras haber sobrevivido a mi ataque cardíaco. Él es jefe de seguridad en Lockheed Martin y también ha estado bajo muchas presiones. Fue muy presionado por su afiliación conmigo," dice Newsham.

Ahora vive sola, y ha luchado por mantener el contacto con sus tres hijos y sus seis nietos. Hoy, vive en un silencioso suburbio de Las Vegas. Ni siquiera sus vecinos tienen idea sobre su pasado.

"Las actividades de la NSA no sólo me han afectado a mí, sino también a mis colegas de espionaje en Lockheed. Cerca de la mitad de la gente con quien trabajé en proyectos clandestinos están o muertos o mortalmente enfermos hoy. Por ejemplo, mi jefe en el proyecto Echelon, Robert Looper, murió prematuramente de ataque al corazón, y Kay Nickerson, quien trabajó en el desarrollo del bombardero Stealth, murió de daño cerebral."

¿Pero cómo pudieron morir prematuramente la mitad de sus compañeros?

"No sé como explicarlo, pero hubo un punto en que descubrimos que el cuartel general de Lockheed en Sunnyvale está construido sobre un lugar de volcado de residuos altamente radioactivos."

¿De qué murieron?

"Ataque al corazón, cáncer, ataques apopléjicos inexplicables y daños en el cerebro. Incluso yo voy a morir de cáncer antes de tiempo. Pero tengo a mis abogados, a mi doctor y a mis hijos y nietos para ayudarme. Son la gente a quien tengo cariño."

¿Qué le da el coraje para continuar?

"El hecho de que la NSA, la CIA y el NRO (National Reconnaissance Organization) están llevando adelante espionaje ilegal contra el resto del mundo. Dicen que lo hacen para coger a narcotraficantes, terroristas, etc. Pero eso no les da el derecho de hacer lo que están haciendo. Están rompiendo constantemente la ley."

ECHELON EN DINAMARCA

En Dinamarca, los líderes políticos y ministros niegan cualquier conocimiento acerca de Echelon más allá de lo que han leído en los periódicos.

"Ahora pueden leer sobre mí entonces. Soy la prueba viviente de la existencia de Echelon. Configuré y usé muchos programas de Echelon.". Margaret Newsham nos muestra la orden que la envió a Menwith Hill, las especificaciones de algunos programas de Echelon y otros documentos internos.

Encontramos restos de ordenadores en el Puesto de Escucha de Aflandshage en Dinamarca designados "VAX RED". ¿Significa esto algo para usted?

"Sí, de hecho significa dos cosas. Trabajaba en VAX personalmente, y se usaban en el proyecto Echelon.

"El color rojo (RED) se refiere probablemente al nivel de clasificación. Dado que el sistema de seguridad se basa en el hecho de que sólo unos pocos tienen una idea de todo lo que sucede. Así, algunos empleados tienen códigos rojos, algunos morados, algunos azules, y así. Eso significa que sólo se les permite trabajar con ciertas partes de los proyectos, por ejemplo, los que están clasificados bajo el mismo color. Como resultado, pocos empleados tienen una idea completa acerca de lo que realmente está sucediendo. Dado que mi etiqueta tenía todos los colores, tengo una buena visión sobre todo. También era quien hacía los backups."

EL GRAN HERMANO TE VIGILA

¿Puedes entender por qué alguna gente encuentra difícil creer que un sistema como éste realmente existe?

"Sí, pero es real. Estamos espiando en nuestros propios ciudadanos y al resto del mundo – incluso a nuestros aliados en Europa. Si digo "Amnistía" o "Margaret Newsham", es interceptado, analizado, coordinado, reenviado y registrado – si es de interés para las agencias de inteligencia. Hablé con un experto en radio recientemente, que había hecho exactamente lo que yo, tan sólo diez años después, en 1991, bajo la "Operación Tormenta del Desierto". Si pudiera decírtelo todo, entonces entenderías que Echelon es tan grande, que su inmensidad hace casi imposible su comprensión." Margaret Newsham no agradece el haber sido una paria en la comunidad de inteligencia de EEUU desde que rompió con la NSA en 1984. Una ruptura que le costó su marido, su trabajo y su salud.

¿Hay algo que hubieras hecho de otra manera?

"No. Es importante que la verdad salga fuera. No creo que debamos de levantarnos al ser controlados por el "Gran Hermano" en el futuro. Deberíamos de levantarnos contra ello ahora."

HECHOS "EXTRA"

Durante 10 años, Newsham trabajó para la firma de ordenadores y municiones de EEUU Signal Science, Ford Aeroespacial, y Lockheed Martin. Tenían contratos para el desarrollo y actualización de los satélites de Echelon y ordenadores que las compañías diseñaron para la agencia NSA. La NSA coopera de modo cercano con la CIA y el NRO (National Reconnaissance Organization). Durante dos años, Newsham compartió la responsabilidad del funcionamiento día a día de la red de ordenadores de Echelon en Menwith Hill, Inglaterra.

En documentos clasificados, que están en posesión de *Ekstra Bladet*, Menwith Hill es mencionada como "la mayor estación en servicio".

Dinamarca participa como tercero en UKUSA, un acuerdo de intercambio electrónico.

17 de Noviembre de 1999

Fuente: http://personal5.iddeo.es/wintrmute/cyberpunk/baby-es.htm

BIBLIOGRAFIA

1. Alem, Jean Pierre "El espionaje y el contraespionaje" Traduc. David Huerta, Ed. Fondo de Cultura Económica, México, 1983, 142 pp.

2. Arenal, Celestino del "Introducción a las Relaciones Internacionales", Ed. Tecnos, 1ra reimpresión, México, 1995, 480 pp.

3. Barrios Garrido, Gabriela "Internet y derecho en México" Ed. McGraw-Hill, México, 1998, 180 pp.

4. Boar, Roger "Los espías y maestros del espionaje más grandes del mundo" Traduc. Luz Broissin, Ed. Edivisión, México, 1996, 269 pp.

5. Brown, Juan "Esbozo de Historia Universal" Ed. Grijalbo, México, 1973, 276 pp.

6. Elliott, Chris "*The legality of the interception of electronic communications*" 28 March 1999.

7. Emilio, Abraham "Lo mejor del espionaje internacional" Ed. Diana, 1996, 498 pp.

8. Fernez, Andri. *El espionaje por dentro*. Traduc. Josi Baeza, Ed. Juventud, Barcelona, 1968, 171 pp.

9. Flores, Olea "Internet y la revolución cibernética" Ed. Océano, 1997, 140 pp.

10. Francoz, Rigalt Antonio, "Derecho Aeroespacial", Ed. Porrua, 1ra Edición, México, 1981, 212 pp.

11. Guillaumin, Claude "Los grandes enigmas del espionaje" Ed. Ferni, 1973. Hance, Oliver "*Leyes y negocios en Internet*" Traduc. Yazmín Parra. Ed. McGraw-Hill, México, 1996, 371 pp.

12. Hinchley, Vernon "Espionaje al desnudo" Traduc. T. de Tovar, Ed. Novaro, México, 1967, 283 pp.

13. Hougan, Jim "Cazadores de secretos", Ed. México Lasser, 1979, 486 pp.

14. Lachs, Manfred "El Derecho del Espacio Ultraterrestre", Fondo de Cultura Económica, Madrid 1977, 195 pp.

15. Levy, Steven "Internet 95", en Newsweek, Nueva York, 25 de diciembre de

1995/1 de enero de 1996.

16. Matterlart, Armand, "*Agresión desde el espacio, cultura y NAPALM en la era de los satelites*" Ed. Siglo XXI, 6ª. Edición, México, 1978, 200 pp.

17. Maureen, Williams Silvia "Derecho Internacional Contemporáneo", Ed. Abeledo-Perrot, Buenos Aires, 1990, 250 pp.

18. Maureen, Williams Silvia, "Telecomunicaciones por satélites" Ed. Abeledo-Perrot, Buenos Aires, 1981, 85 pp.

19. Seara Vázquez, Modesto, "Derecho y Política en el Espacio Cósmico", Universidad Nacional Autónoma de México, 2da edición, México, 1986, 164 pp.

20. Seara Vázquez, Modesto, "Introducción al Derecho Internacional Cósmico", Escuela Nacional de Ciencias Políticas y Sociales, 1ra Edición, México, 1961, 333 pp.

21. Singer, Kurt D. *Espionaje*. Ed. Diana, México, 1961, 186 pp.

22. Toffler, Alvin y Heidi, "Las Guerras del Futuro", Ed. Plaza & Janes, 1ra. Edición, España, 1994, 388 pp.

23. Vásquez, John A. "Relaciones Internacionales", Ed. Limusa, 2da Edición, México, 1994, 406 pp.

24. Verplaetse, Julian G., "Derecho Internacional Aéreo y del Espacio", Ediciones Atlas, Madrid, 1963, 561 pp.

25. Biblioteca de Consulta Microsoft® Encarta® 2003. © 1993-2002 Microsoft Corporation.

FUENTES ELECTRONICAS

1. http://www.aclu.org/Privacy/Privacy.cfm?ID=8476&c=130
2. http://www.aclu.org/safeandfree/
3. http://alainet.org/active/show_text.php3?key=1453
4. http://www.albertverges.com/E_Pintura.htm
5. http://altavoz.nodo50.org/echelon2000.htm
6. http://altavoz.nodo50.org/mas_echelon.htm
7. http://www.apc.org/espanol/news/index.shtml?x=18227
8. http://archive.aclu.org/action/echelon107.html
9. http://www.argenpress.info/nota.asp?num=000195
10. http://www.buenosaires-links.com.ar/memo/recortes/echelon2.htm
11. http://www.buenosaires-links.com.ar/memo/recortes/echelon4.htm
12. http://www.cdt.org/
13. http://ciberhabitat.gob.mx/medios/satelites/artificiales/ -->
14. http://www.ciberpais.elpais.es/d/20010913/cibersoc/soc1.htm
15. http://www.cipherwar.com/echelon/
16. http://civilliberty.about.com/
17. http://colombia.analitica.com/internacionales/1874890.asp
18. http://www.cosmopediaonline.com/sputnik.html -->
19. http://cryptome.org/echelon-cinsa.htm
20. http://csf.colorado.edu/mail/elan/2001/msg00532.html
21. http://www.cyber-rights.org/interception/echelon/

22. http://derechos.apc.org/

23. http://www.derechos.org/nizkor/espana/doc/echelon5sep01.html

24. http://www.diarioti.com/noticias/1999/oct99/15192440.htm

25. http://www.dragones.org/foro/echelon-original.htm

26. http://www.echelon.tsx.org

27. http://www.echelonwatch.org/

28. http://www.enciclopedia.org.uy/autores/HigsKaren/Ciberderechos.htm

29. http://es.geocities.com/jose958/historia_satelites.htm -->

30. http://es.gsmbox.com/news/mobile_news/all/44194.gsmbox

31. http://es.gsmbox.com/news/mobile_news/all/49661.gsmbox

32. http://www.ezln.org/revistachiapas/ch9ornelas.html

33. http://www.fas.org/irp/program/process/echelon.htm

34. http://www.fas.org/irp/program/process/991116-echelon.htm

35. http://www.fas.org/irp/program/process/eu_dissent.html

36. http://fly.hiwaay.net/~pspoole/echelon.html

37. http://fly.hiwaay.net/~pspoole/echres.html

38. http://funredes.org/mistica/castellano/emec/produccion/memoria6/0806.html

39. http://www.galeon.com/futuros/echelon.htm

40. http://www.glosarium.com/term/154,4,xhtml

41. http://www.heise.de/tp/english/inhalt/te/6929/1.html

42. http://www.hq.nasa.gov/office/pao/History/sputnik/sputorig.htm

43. http://iblnews.com/news/noticia.php3?id=22057

44. http://www-istp.gsfc.nasa.gov/Education/Mexp13.html -->
45. http://jya.com/echelon-dc.htm

46. http://jya.com/echelon.htm

47. http://www.lainsignia.org/2001/mayo/cyt_009.htm

48. http://www.lainsignia.org/2001/noviembre/cyt_003.htm

49. http://www.lainsignia.org/ddhh.html

50. http://www.libertaddigital.com:83/ilustracion_liberal/articulo.php/389

51. http://www.mail-archive.com/direitos-humanos@grupos.com.br/msg00606.html

52. http://mediafilter.org/caq/echelon/

53. http://www.memoria.com.mx/157/Resolucion.htm

54. http://www.noticias.com/noticias/2001/0108/n0108032.htm

55. http://www.noticias.com/noticias/2001/0109/n01090651.htm

56. http://www.nsa.gov/about_nsa/index.html

57. http://ofdnews.com/comentarios/63_0_1_0_C/

58. http://www.ociojoven.com/article/articleview/402396/1/216/

59. http://perso.wanadoo.fr/metasystems/ES/BigBrother.html

60. http://personal5.iddeo.es/wintrmute/cyberpunk/baby-es.htm

61. http://www.proyectopv.org/1-verdad/echelon.htm

62. http://public.srce.hr/~mprofaca/echelon01.html

63. http://www.rebelion.org/cibercensura/echelon071102.htm

64. http://www.rnw.nl/informarn/html/act010315_echelon.html

65. http://www.rnw.nl/informarn/html/act010605_echelon.html

66. http://www.seprin.com/echelon27-08-01/echelon.htm

67. http://www.seprin.com/informes/stoa-atpc.htm
68. http://www.seprin.com/perturba_echelon.htm

69. http://www.seprin.com/virus_logico.htm

70. http://serendipity.magnet.ch/hermetic/crypto/echelon/echelon.htm

71. http://www.solidaridad.net/vernoticia.asp?noticia=467

72. http://www.terra.es/personal/fcyborg/ideologia/echelon.htm

73. http://www.tlm.unavarra.es/asignaturas/bi/bi99_00/mejores/bi22/paginas/histor/enfh.htm

74. http://www.ucm.es/info/solidarios/ccs/articulos/medios/echelon_la_tecnologia_avanza_al_servicio_del_autoritarismo.htm

75. http://www.ulpiano.com/bolpriv_Echelon.htm

76. http://www.uned.es/ntedu/espanol/master/primero/modulos/teoria-de-la-informacion-y-comunicacion-audiovisual/mikel-usabiaga-1/el-mundo/Espionaje.htm

77. http://www.uned.es/ntedu/espanol/master/primero/modulos/teoria-de-la-informacion-y-comunicacion-audiovisual/mikel-usabiaga-1/el-mundo/Internet-Denuncias.htm

78. http://www.virusprot.com/Nt150322.html

79. http://www.zdnet.co.uk/news/specials/2000/06/echelon/