PARLAMENTO EUROPEO

1999 *2004*

Comisión temporal sobre el sistema de interceptación ECHELON

PROVISIONAL

18 de mayo de 2001

PROYECTO DE INFORME

sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON)

Comisión temporal sobre el sistema de interceptación ECHELON

Ponente: Gerhard Schmid

ÍNDICE

Página

PÁGINA REGLAMENTARIA

En la sesión del 5 de julio de 2000, el Parlamento Europeo decidió constituir una Comisión temporal sobre el sistema de interceptación ECHELON. Para cumplir su mandato, la comisión temporal, en su reunión constituyente del 5 de junio de 2000, designó ponente al Sr. Gerhard Schmid.

En la reunión del ##, la comisión examinó el proyecto de informe.

En esta última reunión/En la última de estas reuniones, la comisión aprobó la propuesta de resolución por ... votos a favor, ... voto(s) en contra y ... abstención(es)/por unanimidad.

Estuvieron presentes en la votación los diputados: ... (presidente(a)/presidente(a) en funciones), ... (vicepresidente(a)), ... (vicepresidente(a), ... (ponente), ..., ... (suplente de ...), ... (suplente de ... de conformidad con el apartado 2 del artículo 153 del Reglamento), ... y ... .

El informe se presentó el ##.

El plazo de presentación de enmiendas a este informe figurará en el proyecto de orden del día del período parcial de sesiones en que se examine/vencerá a las … horas.

PROPUESTA DE RESOLUCIÓN

Resolución del Parlamento Europeo sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON)

El Parlamento Europeo,

- Vista la Decisión del Parlamento Europeo de 5 de julio de 2000 por la que se constituye una comisión temporal sobre el sistema de interceptación ECHELON y visto el mandato otorgado a la misma,

- Visto el Tratado CE, en el que se proclama el objetivo de realizar un mercado común con un alto grado de competitividad,

- Visto el Tratado de la Unión Europea, y en particular el apartado 2 de su artículo 6, en el que se declara el compromiso de la Unión Europea en favor del respeto de los derechos fundamentales, y visto su título V, que contiene disposiciones relativas a la política exterior y de seguridad común,

- Vista la Carta de los derechos fundamentales de la Unión Europea, en cuyo artículo 7 se proclama el derecho al respeto de la vida privada y familiar y, de manera expresa, el derecho al respeto de las comunicaciones,

- Visto el Convenio Europeo para la protección de los Derechos Humanos y, en particular, su artículo 8, en el que se proclama el derecho al respeto de la esfera privada, y vistos los numerosos acuerdos internacionales en los que se consagra el principio de la protección de la vida privada y familiar,

- Visto el informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema ECHELON), elaborado por la Comisión temporal sobre el sistema de interceptación ECHELON (A5-…./2001),

La existencia de un sistema mundial de interceptación de las comunicaciones privadas y económicas (sistema de interceptación ECHELON)

A: Considerando que no hay ninguna razón para seguir dudando de la existencia de un sistema de interceptación de las comunicaciones a nivel mundial en el que participan los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda en el marco del Acuerdo UKUSA; considerando, asimismo, que según las informaciones de que se dispone, es probable que su nombre sea realmente "ECHELON", si bien no es éste un aspecto de importancia primordial,

B. Considerando que el sistema no se utiliza para interceptar comunicaciones militares, sino privadas y económicas, pero que el análisis presentado en el informe ha mostrado que la potencia de este sistema no puede ser, ni mucho menos, tan grande como se ha supuesto, en parte, en los medios de información,

Los límites del sistema de interceptación

C. Considerando que el sistema de interceptación se basa en la interceptación a escala mundial de las comunicaciones por satélite, aunque en en las regiones con una densidad elevada de comunicaciones el porcentaje de las realizadas por satélite es muy limitado, lo que implica que la mayor parte no pueden interceptarse desde estaciones terrestres, sino mediante la interceptación de cables o de ondas, lo que a su vez -como han puesto de manifiesto las investigaciones efectuadas para la elaboración de este informe- sólo es posible dentro de límites muy estrechos; considerando, además, que los recursos de personal necesarios para la interpretación final de las comunicaciones interceptadas añade otras limitaciones; considerando que, por lo tanto, los Estados ECHELON sólo tienen acceso a una proporción muy reducida de las comunicaciones por cable y por ondas y sólo pueden interpretar una proporción muy escasa de las comunicaciones,

La posible existencia de otros sistemas de interceptación

D. Considerando que, teniendo en cuenta que la interceptación de las comunicaciones en un medio de espionaje tradicional de los servicios de inteligencia, otros Estados también podrían utilizar un sistema similar si dispusieran de los recursos financieros y de las condiciones geográficas adecuadas; considerando que, gracias a los territorios de ultramar de los que dispone, Francia sería, por lo menos en lo que se refiere a las condiciones geográficas, el único Estado miembro de la UE en condiciones de establecer un sistema de interceptación mundial; considerando, además, que existen indicios que permiten afirmar que Rusia también podría explotar un sistema de estas características,

Su compatibilidad con el Derecho de la UE

E. Considerando que por lo que respecta a la compatibilidad de un sistema de las características del sistema ECHELON con el Derecho de la UE hay que hacer dos precisiones: si el sistema se utilizase exclusivamente para fines de información, no habría ningún tipo de contradicción con el Derecho de la UE, ya que el Tratado CE no aborda las cuestiones relacionadas con las actividades en el ámbito de la seguridad nacional, sino que éstas recaen en el ámbito de aplicación del Título V del Tratado UE (PESC), que en la actualidad no incluye ningún tipo de disposiciones en la materia, por lo que no cabría hablar de infracción; por el contrario, si el sistema se utilizase de manera abusiva para espiar a la competencia, sería incompatible con el principio de lealtad que deben respetar los Estados miembros y con el concepto de un mercado común en el que la competencia es libre, por lo que la participación de un Estado miembro en un sistema de estas características sería incompatible con el Derecho comunitario,

Su compatibilidad con el principio fundamental del respeto a la vida privada (artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales)

F. Considerando que toda interceptación de las comunicaciones supone una injerencia grave en la vida privada de la persona; considerando que en el artículo 8 del Convenio

de referencia se garantiza el respeto a la vida privada y únicamente se permite este tipo de intervenciones cuando se trata de garantizar la seguridad nacional y siempre que las normas por las que se rigen estén previstas en el Derecho nacional, sean accesibles a todos y precisen en qué circunstancias y bajo qué condiciones pueden efectuarlas las autoridades; considerando, además, que tales intervenciones deben ser proporcionadas, por lo que debe establecerse un equilibrio entre los intereses en juego, ya que según la jurisprudencia del Tribunal Europeo de Derechos Humanos no es suficiente que estas medidas sean necesarias o deseables,

G. Considerando que un sistema de inteligencia que interceptase todos los mensajes faltando al principio de proporcionalidad sería contrario al Convenio Europeo de Derechos Humanos, como también lo sería si las disposiciones en las que se apoyase la interceptación de las comunicaciones no se basasen en un fundamento jurídico, si no fuesen accesibles a todos o si se formulasen de tal modo que sus consecuencias sobre los particulares fuesen impredecibles; considerando que las normas por las que se rigen las actividades de los servicios de inteligencia de los Estados Unidos en el extranjero son secretas en su mayor parte, por lo que en este caso el respeto del principio de proporcionalidad es, cuanto menos, dudoso y es muy probable que dichas normas estén en contradicción con los principios de acceso a la ley y de previsibilidad de sus efectos,

H. Considerando que los Estados miembros no pueden sustraerse a las obligaciones que les impone el Convenio Europeo de Derechos Humanos permitiendo que desarrollen actividad en sus respectivos territorios los servicios de inteligencia de otros Estados que se rigen por normas menos estrictas, puesto que con ello se anularía la eficacia del principio de legalidad, con sus dos componentes de accesibilidad de la ley y previsibilidad de sus efectos, y se vaciaría de contenido la jurisprudencia del Tribunal Europeo de Derechos Humanos,

I. Considerando que para que las actividades jurídicamente legitimadas de los servicios de inteligencia sean compatibles con los derechos fundamentales es necesaria, además, la existencia de suficientes mecanismos de control para contrarrestar los peligros que conllevan las actividades secretas de determinados segmentos del aparato de la Administración; considerando que el Tribunal Europeo de Derechos Humanos ha subrayado expresamente la importancia que revisten unos sistemas de control eficaces en el ámbito de las actividades de los servicios de inteligencia, por lo que resulta preocupante que algunos de los Estados miembros no dispongan de órganos de control parlamentario de los servicios secretos,

El grado de protección de los ciudadanos de la UE frente a los servicios de inteligencia

J. Considerando que la protección de los ciudadanos de la UE depende de la situación jurídica en cada Estado miembro y que ésta es muy distinta entre los diferentes Estados, ya que en algunos casos no existe ningún órgano de control parlamentario y apenas puede hablarse de un grado de protección adecuado; considerando que para los ciudadanos europeos es fundamental que sus Parlamentos nacionales cuenten con una comisión especial de control estructurada que controle y examine las actividades de los servicios de inteligencia; considerando que incluso en los países que cuentan con

tales órganos de control éstos tienden a preocuparse en mayor medida de las actividades de los servicios de inteligencia en el interior del propio territorio que en el exterior, ya que, por regla general, a los ciudadanos del propio país sólo les afectan los primeros,

K. Considerando que en el caso de la cooperación entre servicios de inteligencia en el marco de la PESC, las instituciones tiene el deber de adoptar disposiciones de protección suficientes en beneficio de los ciudadanos europeos,

El espionaje económico

L. Considerando que uno de los componentes de la misión de los servicios de inteligencia en el exterior es interesarse por los datos económicos tales como el desarrollo de los distintos sectores, la evolución de los mercados de materias primas, el respeto de los embargos económicos, el cumplimiento de las disposiciones relativas al suministro de productos de doble uso, etc., y que por esta razón se vigila con frecuencia a las empresas activas en estos ámbitos,

M. Considerando que, en cualquier caso, no puede tolerarse que los servicios de inteligencia se dejen instrumentalizar para espiar a la competencia y sometan a observación a las empresas extranjeras a fin de lograr ventajas competitivas para las empresas nacionales, si bien, a pesar de las muchas afirmaciones que se han hecho en tal sentido, no existen pruebas de ésta haya sido la razón por la que se creó en sistema mundial de interceptación de comunicaciones,

N. Considerando que en muchos casos las informaciones sensibles relativas a las empresas se encuentran en las propias empresas, de modo que el espionaje para la competencia consiste, en primer lugar, en obtener información a través de los empleados o de personas infiltradas o entrando en las redes informáticas internas; considerando que los sistemas de interceptación de comunicaciones para el espionaje industrial sólo pueden utilizarse cuando las informaciones sensibles se transmiten al exterior por cable o por ondas (satélite), lo que se sólo se hace de manera sistemática en los tres casos siguientes:

- cuando las empresas trabajan en las tres franjas horarias, de modo que los resultados parciales correspondientes a Europa se transmiten a América y, a continuación, a Asia;
- cuando los consorcios internacionales celebran videoconferencias por satélite de telecomunicaciones o por cable;
- cuando se negocian in situ contratos importantes (por ejemplo, construcción de plantas industriales, infrastructuras de telecomunicaciones, construcción de sistemas de transporte, etc.) y es necesario consultar con la sede central de la empresa .

La posibilidad de autoprotección

O. Considerando que las empresas sólo pueden alcanzar el grado de seguridad necesario cuando está protegido todo el entorno de trabajo, al igual que todos los canales de comunicación por los que se transmiten informaciones sensibles; considerando que en

el mercado europeo existen sistemas de encriptación que ofrecen un grado de seguridad suficiente a precios asequibles; considerando que también se debe instar a los particulares a que cifren el correo electrónico, ya que un mensaje sin cifrar es como una carta sin sobre; considerando que en Internet se ofrecen para ello sistemas relativamente fáciles de utilizar y que algunos de ellos pueden obtenerse gratuitamente, incluso, para uso privado,

La cooperación de los servicios de inteligencia en el seno de la UE

P. Considerando que la UE ha acordado coordinar las actividades de obtención de información de sus servicios en el marco del desarrollo de una política propia de seguridad y defensa, así como continuar su colaboración con otros socios,

Q. Considerando que la cooperación entre los servicios de inteligencia existentes en la UE resulta deseable toda vez que, por una parte, una política de seguridad común que excluyese los servicios de inteligencia no tendría sentido y, por otra, dicha cooperación implicaría numerosas ventajas desde el punto de vista profesional, financiero y político; considerando, además, que se correspondería mejor con la idea de una UE como socio en pie de igualdad de los Estados Unidos y permitiría reagrupar al conjunto de los Estados miembros en un sistema plenamente compatible con el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales; considerando que, en tal caso, debería garantizarse que el Parlamento Europeo pudiese ejercer el control que le corresponde,

R. Considerando que el Parlamento Europeo está estudiando diversas reglamentaciones relativas al acceso a informaciones y documentos confidenciales y sensibles,

La celebración y la modificación de tratados internacionales sobre la protección de los ciudadanos y de las empresas

1. Insta al Secretario General del Consejo de Europa a que presente al Comité de Ministros un estudio sobre la conveniencia de adaptar a los métodos de comunicación y a las posibilidades de interceptación existentes en la actualidad las disposiciones del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales que garantizan la protección de la vida privada en un protocolo adicional o conjuntamente con las disposiciones relativas a la protección de los datos en el marco de una revisión de la Convención relativa a la protección de la información, con la condición de que ello no se traduzca en una reducción del nivel de protección establecido por el Tribunal ni en una reducción de la flexibilidad necesaria para adaptarse a futuros cambios de la situación;

2. Insta a los Estados miembros a que creen una plataforma europea para examinar las disposiciones legales relativas al respeto del secreto postal y de las comunicaciones, a que lleguen a un acuerdo sobre un texto común que garantice a todos los ciudadanos europeos que residan en el territorio de los Estados miembros la protección de la vida privada proclamada como derecho en el artículo 7 de la Carta Europea de los Derechos Fundamentales y que, además, garanticen que los servicios de inteligencia desarrollen sus actividades en el respeto de los derechos fundamentales, de modo que

se correspondan con las disposiciones recogidas en el capítulo 8 del presente informe, en particular en el apartado 8.3.4, y derivadas del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales;

3. Pide a los Estados miembros del Consejo de Europa que adopten un protocolo adicional que permita la adhesión de las Comunidades Europeas al Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales o que reflexionen sobre otras medidas que eviten conflictos de jurisdicción entre los Tribunales de Estrasburgo y de Luxemburgo;

4. Insta al Secretario General de las Naciones Unidas a que encargue a la comisión competente la presentación de propuestas que adapten a la evolución tecnológica el artículo 17 del Pacto Internacional sobre los derechos cívicos y políticos, que protege la vida privada;

5. Insta a los Estados Unidos a firmar el Protocolo adicional al Pacto internacional sobre los derechos cívicos y políticos, de modo que se puedan presentar ante la Comisión de Derechos Humanos creada en aplicación del Convenio las quejas presentadas por particulares contra los Estados Unidos por violación de este Pacto; pide a las ONG de los Estados Unidos pertinentes, en particular a la ACLU (American Civil Liberties Union) y al EPIC (Electronic Privacy Information Center) que ejerzan presiones ante el Gobierno estadounidense en este sentido;

Las disposiciones legislativas nacionales de protección de los ciudadanos y de las empresas

6. Insta a todos los Estados miembros a que examinen su propia legislación en relación con la conformidad de las actividades de los servicios de inteligencia con los principios fundamentales;

7. Pide a los Estados miembros que se propongan como objetivo un nivel de protección común frente a las actividades de los servicios de inteligencia tomando como referencia por el mayor grado de protección que exista en los Estados miembros, ya que, por regla general, los afectados por las actividades de un servicio de inteligencia exterior son los ciudadanos de otro Estado y, por consiguiente, también los de otros Estados miembros;

8. Insta a las instituciones de la UE a que, en caso de que los servicios de inteligencia cooperen en el marco de la PESC, adopten disposiciones de protección de los ciudadanos europeos en grado suficiente; por su parte, el Parlamento Europeo, como órgano lógico de control, deberá crear las condiciones necesarias para supervisar este ámbito tan sensible, de modo que pueda reivindicar las correspondientes facultades de control de forma realista y responsable;

Las medidas jurídicas concretas de lucha contra el espionaje industrial

9. Pide a los Estados miembros que examinen hasta qué punto la adopción de disposiciones de derecho europeo e internacional puede servir para luchar contra el espionaje industrial y el soborno y, en particular, si es posible establecer una

normativa en el marco de la OMC que tenga en cuenta el impacto negativo de este tipo de acciones sobre la competencia y que, por ejemplo, permita declarar nulos los contratos celebrados en estas circunstancias;

10. Pide a los Estados miembros que, con una declaración común formulada en términos inequívocos, se comprometan a no realizar espionaje industrial recíproco y, de este modo, den muestras de su voluntad de respetar el espíritu y la letra del Tratado CE;

Las medidas jurídicas de aplicación y su control

11. Hace un llamamiento a los Parlamentos nacionales que no cuentan con ningún tipo de órgano de control parlamentario encargado del control de los servicios de inteligencia a que adopten las medidas necesarias para su creación;

12. Insta a las comisiones nacionales de control de los servicios de inteligencia a que al ejercer sus competencias en materia de control concedan gran importancia a la protección de la vida privada, independientemente de que se trate de la vigilancia de ciudadanos del propio Estado, de otros ciudadanos de la UE o de ciudadanos de terceros países;

13. Pide a Alemania y al Reino Unido a que en el futuro sólo autoricen la interceptación de las comunicaciones por parte de los servicios de inteligencia de los Estados Unidos en su territorio si en esta actividad se respeta el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, es decir, si se respeta el principio de proporcionalidad, si su fundamento jurídico es accesible y si sus repercusiones sobre los individuos son previsibles, y que establezcan un control eficaz en este sentido, ya que son responsables de que las actividades de obtención de información desarrolladas por los servicios de inteligencia en su territorio, independientemente de que estén autorizadas o únicamente toleradas, están en conformidad con el imperativo del respeto de los derechos humanos ;

Las medidas de impulso de la autoprotección de los ciudadanos y de las empresas

14. Insta a la Comisión y a los Estados miembros a que desarrollen programas que fomenten el grado de conciencia de los ciudadanos y de las empresas en relación con los problemas relacionados con la seguridad y, al mismo tiempo, a que brindan asistencia práctica para la concepción y la aplicación de sistemas completos de protección;

15. Pide a la Comisión y a los Estados miembros que adopten medidas adecuadas para impulsar, desarrollar y producir tecnologías y programas informáticos europeos de encriptación y, en particular, que apoyen proyectos que tengan como objetivo el desarrollo de programas de encriptación fáciles de usar y cuyo código fuente sea público;

16. Insta a la Comisión y a los Estados miembros a que fomenten los proyectos de programas informáticos de código abierto, ya que éste es el único modo de garantizar que no ofrezcan "puertas traseras" que puedan hacerlos vulnerables;

17. Insta a las instituciones europeas y a las administraciones públicas de los Estados miembros a que encripten sistemáticamente sus mensajes electrónicos para que, a la larga, esta práctica se convierta en norma habitual;

Otras medidas

18. Insta a las empresas a que colaboren más estrechamente con los servicios de contraespionaje y que, en particular, les comuniquen los ataques procedentes del exterior con fines de espionaje industrial, para aumentar el grado de eficacia de estos servicios;

19. Pide a la Comisión que presente una propuesta de creación de una oficina europea de asesoramiento en materia de seguridad de la información empresarial que tenga como misión elevar el grado de sensibilización ante el problema y proporcionar ayuda práctica;

20. Considera conveniente organizar un congreso internacional, no limitado a Europa, sobre la protección de la vida privada frente a la interceptación de las telecomunicaciones, con el fin de crear una plataforma en la que las ONG europeas, de los Estados Unidos y de otros Estados puedan debatir aspectos transfronterizos e internacionales y coordinar ámbitos de actuación y procedimientos;

21. Encarga a su Presidenta que transmita la presente resolución al Consejo, a la Comisión y a los Gobiernos y Parlamentos de los Estados miembros, así como a los países candidatos a la adhesión y al Consejo de Europa.

EXPOSICIÓN DE MOTIVOS

1. Introducción

1.1. El motivo de la constitución de la comisión temporal

El 5 de julio de 2000, el Parlamento Europeo decidió constituir una comisión temporal sobre el sistema de interceptación ECHELON. Esta decisión se adoptó a raíz del debate sobre el estudio encargado por STOA[1] en relación con el denominado sistema ECHELON[2], que su autor, Duncan Campbell, había presentado con ocasión de una audiencia de la Comisión de Libertades y Derechos de los Ciudadanos, Justicia y Asuntos Interiores, sobre la Unión Europea y la protección de los datos.

1.2. Las afirmaciones hechas en los dos estudios de STOA sobre un sistema mundial de interceptación de comunicaciones con el nombre clave de ECHELON

1.2.1. El primer informe STOA de 1997

En un informe sobre el tema "Evaluación de las tecnologías de control político" encargado en 1997 por STOA[3] a la Fundación Omega para el Parlamento Europeo se describía el sistema ECHELON, concretamente en el capítulo dedicado a las redes nacionales e internacionales de vigilancia de las comunicaciones. En dicho estudio, el autor afirmaba que dentro de Europa la Agencia Nacional de Seguridad (NSA, servicio de inteligencia exterior de los Estados Unidos) intercepta[4] de manera habitual todas las comunicaciones de correo electrónico, teléfono y fax. Aquel informe hizo que en toda Europa se conociera la existencia de ECHELON como presunto sistema de interceptación de la totalidad de las comunicaciones.

1.2.2. Los informes STOA de 1999

Par obtener más conocimientos en esta materia, STOA encargó en 1999 un estudio dividido en cinco partes sobre el tema "Desarrollo de la tecnología de vigilancia y riesgos de uso indebido de la información económica". En el volumen 2/5, redactado por Duncan Campbell, se estudiaban las capacidades de interceptación e información existentes por aquellas fecha y, en particular, el modo de funcionamiento de ECHELON.[5]

---

[1] STOA (Scientific and Technological Options Assessment): servicio de la Dirección General de Estudios del Parlamento Europeo que encarga trabajos de investigación.

[2] Estado actual de la tecnología en el ámbito de las actividades de espionaje de las comunicaciones (COMINT) para el procesado automatizado con fines de espionaje de sistemas de banda ancha multilingües interceptados, pertenecientes a operadores de redes propias o arrendadas, y su utilidad para la búsqueda y selección de objetivos COMINT, incluido el reconocimiento de voz (octubre de 1999).

[3] Scientific and Technological Options Assessment.

[4] Steve Wright, An appraisal of technologies for political control (1998), p. 20.

[5] Estado actual de la tecnología en el ámbito de las actividades de espionaje de las comunicaciones (COMINT) para el procesado automatizado con fines de espionaje de sistemas de banda ancha multilingües interceptados, pertenecientes a operadores de redes propias o arrendadas, y su utilidad para la búsqueda y selección de objetivos COMINT, incluido el reconocimiento de voz (octubre de 1999), PE 168.184.

Causó especial expectación la afirmación contenida en el informe en el sentido de que ECHELON se había apartado de su objetivo original de defensa frente a las potencias del Este y se dedicaba en la actualidad al espionaje económico. En el informe la tesis se reforzaba con ejemplos de presunto espionaje económico; en particular, se afirmaba que las sociedades Airbus y Thompson CFS habían resultado perjudicadas por tales actividades.

Como consecuencia del estudio STOA, el asunto ECHELON se examinó en casi todos los Parlamentos de los Estados miembros; en Francia y Bélgica se elaboraron incluso informes sobre este tema.

1.3. El mandato de la comisión temporal

Además de la decisión de constituir una comisión temporal, el Parlamento Europeo aprobó el mandato de la misma. Según dicho mandato, la comisión temporal tiene la misión de:

"- comprobar la existencia del sistema de interceptación de comunicaciones conocido por el nombre de ECHELON, cuyo funcionamiento se describe en el informe STOA sobre el desarrollo de la tecnología de vigilancia y los riesgos de mal uso de la información económica;

- evaluar la compatibilidad de dicho sistema con la legislación comunitaria, en particular con el artículo 286 del Tratado CE y las Directivas 95/46/CE y 97/66/CE, y con el apartado 2 del artículo 6 del Tratado de la Unión Europea, a la luz de las cuestiones siguientes:

- ¿Están protegidos los derechos de los ciudadanos europeos frente a las actividades de los servicios secretos?

- ¿Es la encriptación un medio de protección adecuado y suficiente para garantizar la integridad de la vida privada de los ciudadanos, o deben adoptarse medidas adicionales para lograr este fin? En tal caso, ¿qué clase de medidas?

- ¿Cómo se puede reforzar la conciencia de las instituciones europeas sobre los riesgos que encierran estas actividades y qué medidas pueden adoptarse al respecto?

- determinar si la industria europea está expuesta a riesgos como consecuencia de la interceptación global de las comunicaciones;

- formular, si procede, propuestas de iniciativas políticas y legislativas."

1.4. ¿Por qué no una comisión temporal de investigación?

El Parlamento Europeo se decidió por constituir una comisión temporal porque la constitución de una comisión de investigación sólo está prevista para examinar infracciones del Derecho comunitario en el marco del Tratado CE (artículo 193 del Tratado CE) y, en consecuencia, esta clase de comisiones sólo puede ocuparse de los asuntos contemplados en aquella disposición. Los asuntos contemplados en el Título V del Tratado UE (PESC) y VI del mismo Tratado (cooperación policial y judicial en materia penal) están excluidos de las posibles competencias

de las comisiones de investigación. Además, de conformidad con la decisión[6] interinstitucional en esta material, las atribuciones especiales de una comisión de investigación por lo que se refiere a mandatos de comparecencia de funcionarios o acceso a documentos sólo se otorgan cuando no se oponen a ellas consideraciones de necesidad de secreto o de seguridad pública o nacional, lo que excluye, en cualquier caso, la posibilidad de exigir la comparecencia de miembros de servicios de inteligencia. Además, una comisión de investigación no puede extender su actividad a terceros países, ya que éstos, por definición, no pueden infringir el Derecho comunitario. Así, la constitución de una comisión de investigación sólo habría significado una limitación de los contenidos sin aumento de las atribuciones, por lo que la mayoría de los diputados al Parlamento Europeo rechazaron esta fórmula.

1.5. El método y el programa de trabajo

Para ejecutar a plena satisfacción su mandato, la comisión temporal optó por proceder de la forma que expone a continuación. En un programa de trabajo propuesto por el ponente y aprobado por la comisión se presentaba la siguiente lista de ámbitos temáticos relevantes: 1) Datos comprobados sobre ECHELON; 2) Debates al nivel de los Parlamentos y Gobiernos nacionales; 3) Los servicios de inteligencia y sus actividades; 4) Los sistemas de comunicación y la posibilidad de interceptarlos; 5) Cifrado; 6) Espionaje económico; 7) Objetivos de espionaje y medidas de protección; y 8) Condiciones jurídicas marco y protección de la vida privada. Los temas se examinaron de forma consecutiva en las distintas reuniones, orientándose el orden por puntos de vista prácticos, sin que supusiera ningún juicio sobre la importancia de los distintos ámbitos temáticos. Como parte de la preparación de cada reunión, el ponente examinó y evaluó sistemática el material disponible. Después, y en función de las exigencias de cada ámbito temático, se invitó a las reuniones a representantes de las Administraciones nacionales (en particular de los servicios de inteligencia) y de los Parlamentos, en su función de órganos de control de los servicios de inteligencia, así como a expertos del ámbito del Derecho y de los ámbitos de la técnica de comunicación e interceptación, la seguridad empresarial y la criptografía, tanto del terreno científico como del práctico. Las reuniones fueron, en general, públicas, aunque en ocasiones también se celebraron reuniones a puerta cerrada, cuando ello pareció aconsejable para la obtención de información. Además, el presidente de la comisión temporal y el ponente se desplazaron conjuntamente a Londres y París para reunirse allí con personas que, por distintos motivos, no podían participar en las reuniones de la comisión, pero cuya participación en los trabajos de la comisión parecía aconsejable. Por las mismas razones, la Mesa de la comisión temporal, los coordinadores y el ponente viajaron a los Estados Unidos. Además, el ponente mantuvo numerosas entrevistas individuales, en parte de carácter confidencial.

1.6. Las propiedades atribuidas al sistema ECHELON

El sistema de interceptación denominado ECHELON se distingue de los otros sistemas de inteligencia en dos propiedades que le confieren características muy peculiares:
En primer lugar, se le atribuye la capacidad de ejercer una vigilancia simultánea de la totalidad de las comunicaciones. Según se afirma, todo mensaje enviado por teléfono, telefax, Internet o correo electrónico, sea cual sea su remitente, puede captarse mediante estaciones de

[6] Decisión del Parlamento Europeo, del Consejo y de la Comisión, de 19 de abril de 1995, relativa a las modalidades de ejercicio del derecho de investigación del Parlamento Europeo (95/167/CE), artículo 3, apartados 3-5.

interceptación de comunicaciones por satélite y satélites espía, lo que permite conocer su contenido.

Como segunda característica de ECHELON se menciona que este sistema funciona a escala mundial gracias a la cooperación de distintos Estados (el Reino Unido, los Estados Unidos, Canadá, Australia y Nueva Zelanda), lo que significa un valor añadido en comparación con los sistemas nacionales: los Estados que participan en el sistema ECHELON (los Estados ECHELON) pueden ponerse mutuamente a disposición las instalaciones de escucha e interceptación, sufragar conjuntamente los gastos resultantes y utilizar de manera conjunta la información obtenida. Esta cooperación internacional es imprescindible, justamente, para una vigilancia a escala mundial de las comunicaciones por satélite, puesto que sólo de esta manera puede garantizarse que en las comunicaciones internacionales puedan captarse los mensajes de los dos interlocutores en un intercambio. Es evidente que las estaciones de interceptación de comunicaciones por satélite, por sus dimensiones, no pueden construirse en el territorio de un Estado sin el consentimiento de éste. En este terreno es imprescindible el acuerdo mutuo y la cooperación de varios Estados situados en distintos continentes.

Los posibles peligros que un sistema como ECHELON encierra para la esfera privada y la economía no sólo se derivan del hecho de que se trate de un sistema de interceptación especialmente poderoso; más bien se deriva de que este sistema funciona en un ámbito carente, casi por completo, de regulación jurídica. Por lo general, un sistema de interceptación de comunicaciones internacionales no apunta a la población del propio país. Así, la persona objeto de observación, por ser extranjera para el país observador, no dispone de ninguna clase de protección jurídica intraestatal. Por ello, cada persona está en situación de completa indefensión frente a este sistema. El control parlamentario resulta, en este ámbito, igualmente insuficiente, puesto que los electores, que parten de la base de que el problema no les afecta a ellos sino "sólo" a personas que viven en el extranjero, no muestran especial interés en que se controle tal actividad, y sus representantes electos cuidan, en primer lugar, los intereses de sus electores. Así, no es de extrañar que en las audiencias celebradas en el Congreso de los Estados Unidos sobre la actividad de la NSA sólo se examine la cuestión de si estas actividades afectan a ciudadanos de los Estados Unidos, sin que la actividad de tal sistema, en sí, suscite mayores reparos. Por ello es más importante todavía examinar este asunto en el ámbito europeo.

2. La actividad de los servicios exteriores de inteligencia

2.1. Introducción

Para garantizar la seguridad de sus respectivos países, la mayor parte de Gobiernos mantienen, junto a los cuerpos de policía, servicios de inteligencia. Dado que, por lo general, la actividad de estos servicios es secreta, se les denomina también servicios secretos. El cometido de estos servicios es:

- obtener información para alejar peligros para la seguridad del Estado;
- ejercer actividades de contraespionaje en general;
- prevenir riesgos que puedan amenazar a las fuerzas armadas;
- obtener información sobre distintos aspectos de la situación en el extranjero.

2.2. ¿Qué es el espionaje?

Los Gobiernos necesitan reunir y evaluar de forma sistemática información sobre determinados aspectos de la realidad en otros Estados. Se trata de información fundamental para adoptar decisiones en el ámbito de la defensa, de la política exterior, etc. Por ello, los Gobiernos mantienen servicios exteriores de inteligencia. En primer lugar, estos servicios se sirven sistemáticamente de fuentes de información de acceso público. El ponente ha recibido indicaciones en el sentido de que, por término medio, esta vía de información constituye, por lo menos, el 80% de la actividad de los servicios exteriores de inteligencia.[7] Sin embargo, la información de especial importancia en los ámbitos mencionados arriba es mantenida en secreto por los Gobiernos o las empresas y, por ello, no es accesible para el público. Quien, pese a ello, desea disponer de tal información, debe robarla. El espionaje no es más que el robo organizado de información.

2.3. Objetivos del espionaje

Los objetivos clásicos del espionaje son los secretos militares, otros secretos o informaciones gubernamentales sobre la estabilidad o la inestabilidad de los Gobiernos. Ello afecta, por ejemplo, a nuevas armas, estrategias militares o informaciones sobre estacionamientos de tropas. No menos importantes son las informaciones sobre decisiones inminentes en materia de política exterior, política monetaria o información privilegiada sobre tensiones en el seno de un Gobierno. Además, existe también interés en informaciones importantes para la economía. En ellas pueden incluirse, junto a las informaciones propias de una determinada rama de la industria, detalles sobre nuevas tecnologías o negocios en el exterior.

2.4. Los métodos de espionaje

El espionaje significa crear acceso a informaciones cuyo poseedor, en realidad, desea poner fuera del alcance de extraños. Así pues, es necesario burlar o quebrar el dispositivo de protección interpuesto a tal efecto. Ello es así en el espionaje político, tanto como en el espionaje económico. Por ello, para el espionaje se plantean los mismos problemas en los dos terrenos, y

[7] En su informe "Preparing form the 21st Century: An Appraisal of U.S. Intelligence" , la "Comisión de funciones y capacidades de los servicios de inteligencia de los Estados Unidos" señaló que el 95% de la información en materia económica procede de fuentes públicas (Capítulo 2 "The Role of intelligence").

por la misma razón se aplican las mismas técnicas de espionaje en los dos ámbitos. Desde el punto de vista lógico no existe diferencia entre un espionaje y otro; la única diferencia es que, en la economía, el nivel de protección es menor, por lo que, en ocasiones, el espionaje económico resulta de ejecución más sencilla. Otra diferencia señalada es que la conciencia de riesgo entre los usuarios de sistemas de comunicación interceptables es, en el mundo de la economía, menos aguda que en los ámbitos de la seguridad del Estado.

2.4.1. El empleo de personas en el espionaje

La protección de la información secreta se organiza siempre de la misma manera:

- sólo un número limitado de personas de fiabilidad garantizada tienen acceso a la información secreta;
- no existen normas fijas para el manejo de dicha información;
- normalmente, las informaciones no salen del ámbito protegido y, cuando lo hacen, sólo lo hacen por vías seguras o codificadas. Por ello, el espionaje organizado apunta en primer lugar al objetivo de conseguir la información deseada a través de **personas** (la denominada "inteligencia humana"), directamente y sin rodeos. Puede tratarse de:

    - personas infiltradas (agentes) del propio servicio o de la propia empresa;
    - personas captadas en el ámbito en el que se sitúa el objetivo.

Las personas captadas suelen trabajar para servicios o empresas exteriores por los motivos siguientes:

- seducción sexual;
- soborno con dinero o con prestaciones convertibles en dinero;
- chantaje;
- apelación a las ideologías;
- atribución de especial importancia u honor (recurso a los sentimientos de insatisfacción o inferioridad).

Un caso límite es el de la colaboración involuntaria por "absorción". Para ello se aprovecha la vanidad u otras debilidades de miembros del personal de organismos públicos o empresas para hacerles hablar de forma imprudente en situaciones presuntamente inofensivas (conversaciones al margen de conferencias o congresos, o en bares de hotel), etc.

El empleo de personas tiene la ventaja del acceso directo a la información deseada. Sin embargo, también ofrece inconvenientes:

- el contraespionaje se concentra siempre en personas o agentes de enlace y dirección;
- en el caso de las personas captadas, las debilidades que permitieron captarlas pueden volverse en contra de quien las captó (efecto bumerang);
- los seres humanos cometen siempre errores y, por ello, acaban tarde o temprano en la red del contraespionaje.

En la medida de lo posible se intenta, pues, sustituir el empleo de agentes o personas captadas por un espionaje e independiente de cualquier persona. El ámbito en el que esta sustitución

resulta más fácil es en el de la captación y evaluación de señales de radio de instalaciones o vehículos importantes para lo militar.

2.4.2. La interpretación de señales electromagnéticas

La forma más conocida para el gran público de espionaje por medios técnicos es el empleo de la fotografía hecha desde satélites. Pero también se captan e interpretan señales electromagnéticas de todos los tipos (se habla aquí de inteligencia de señales o actividad "SIGINT").

2.4.2.1. Señales electromagnéticas que no sirven a la comunicación

Determinadas señales electromagnéticas, como por ejemplo las radiaciones de estaciones de radar, pueden contener información valiosa en el aspecto militar sobre la organización de la defensa aérea del adversario (se habla aquí de inteligencia electrónica o "ELINT"). Además, las radiaciones electromagnéticas que pueden facilitar información sobre la posición de tropas, aviones, buques o submarinos constituyen una valiosa fuente de información para un servicio de espionaje. También es importante seguir a los satélites espía de otros Estados que toman fotografías y descodificar las señales que emiten.

Las señales son captadas por estaciones terrestres fijas, por satélites en órbita baja o por satélites semiestacionarios SIGINT. Este apartado de la actividad de espionaje relacionada con las señales electromagnéticas constituye una parte importante, desde el punto de vista cuantitativo, de las capacidades de interceptación de los servicios. Pero con ello no se agotan las posibilidades de utilización de la técnica.

2.4.2.2. La interpretación de las comunicaciones interceptadas

Los servicios exteriores de inteligencia de numerosos Estados interceptan las comunicaciones militares y diplomáticas de otros Estados. Muchos de estos servicios vigilan asimismo, en la medida del acceso de que dispongan, las comunicaciones civiles de otros Estados. En determinados países, estos países tienen derecho a vigilar las comunicaciones que entran en el propio país o que salen de él. En los países democráticos, la vigilancia de la comunicación es competencia de los propios ciudadanos, a través de controles y condiciones de intervención impuestos a los servicios de inteligencia. Sin embargo, las legislaciones nacionales sólo protegen a los ciudadanos que se encuentran en el territorio de soberanía del Estado (véase el capítulo 8).

2.5. La actividad de determinados servicios de inteligencia

El principal desencadenante del debate público ha sido la actividad de interceptación desarrollada por los servicios de inteligencia estadounidense y británico. Se ha criticado la escucha, grabación e interpretación de las comunicaciones orales, de fax y de correo electrónico. Para formular una valoración **política** se requiere un criterio de medida para enjuiciar esta actividad. Como término de comparación puede tomarse la actividad de interceptación de comunicaciones de los servicios exteriores de inteligencia dentro de la UE. El cuadro siguiente ofrece una visión general de dicha actividad. De él se desprende que la escucha de comunicaciones privadas por servicios extranjeros no es una especialidad exclusiva de los servicios de inteligencia de los Estados Unidos ni del Reino Unido.

País	Comunicaciones del extranjero	Comunicaciones estatales	Comunicaciones civiles
Bélgica	+	+	-
Dinamarca	+	+	+
Finlandia	+	+	+
Francia	+	+	+
Alemania	+	+	+
Grecia	+	+	-
Irlanda	-	-	-
Italia	+	+	+
Luxemburgo	-	-	-
Países Bajos	+	+	+
Austria	+	+	-
Portugal	+	+	-
Suecia	+	+	+
España	+	+	+
Reino Unido	+	+	+
Estados Unidos	+	+	+
Canadá	+	+	+
Australia	+	+	+
Nueva Zelanda	+	+	+

Cuadro 1: Actividades de interceptación de los servicios de inteligencia en la UE y en los Estados ECHELON

Significado de las columnas:

Columna 1: país
Columna 2: se interceptan las comunicaciones del extranjero
Columna 3: se interceptan las comunicaciones estatales (ejército, embajadas, etc.)
Columna 4: se interceptan las comunicaciones civiles

3. El marco de condiciones técnicas de la interceptación de telecomunicaciones

3.1. El riesgo de interceptación de los distintos medios de comunicación

Cuando las personas desean comunicar entre sí a una distancia determinada, necesitan un medio de comunicación. Este medio puede ser:
- el aire (ondas sonoras);
- la luz (centelleos Morse, cable de fibra óptica);
- la corriente eléctrica (telégrafo, teléfono);
- una onda electromagnética (la señal de radio en sus distintas formas).

Cuando un tercero logra acceder al medio de comunicación, puede interceptar los mensajes que se transmiten por él. El acceso puede ser fácil o difícil, desde cualquier lugar o desde determinadas ubicaciones. En los apartados siguientes se examinan dos casos extremos: las posibilidades técnicas de un espía en el lugar de la comunicación, por una parte, y las posibilidades de un sistema de interceptación que actúe a escala mundial, por otra.

3.2. Las posibilidades de interceptación sobre el terreno[8]

Cualquier comunicación puede ser interceptada sobre el terreno cuando el espía está dispuesto a cometer un delito y el espiado no se protege frente a este riesgo.

- Las **conversaciones** en inmuebles pueden interceptarse con micrófonos introducidos en ellos (micrófonos ocultos) o captando las vibraciones de los cristales de las ventanas con láser.

- Las **pantallas de tubos de rayos catódicos** emiten radiaciones que pueden captarse a una distancia de hasta 30 metros; de este modo se hace visible el contenido de la pantalla.

- El **teléfono**, el **telefax** y el **correo electrónico** pueden interceptarse cuando el espía accede físicamente a los cables que salen de edificio.

- Un **teléfono portátil** puede interceptarse a una distancia de hasta … kilómetros.

- Las **comunicaciones radiofónicas internas de empresa** pueden interceptarse dentro del ámbito de difusión de las ondas ultracortas.

Las condiciones para el empleo de medios técnicos para el espionaje resultan ideales cuando esta actividad se efectúa sobre el terreno, puesto que las medidas de interceptación pueden limitarse a una persona o un objeto y prácticamente pueden captarse todas sus comunicaciones. El único inconveniente es, en el caso de la instalación de un micrófono oculto o de la interceptación física de un cable, un cierto riesgo de que se descubra la maniobra.

[8] Manfred Fink, Lauschziel Wirtschalft - Abhörgefahren und -techniken, Vorbeugung und Abwehr, (La economía como objetivo del espionaje: riesgos y técnicas de la interceptación. Prevención y defensa) Richard Boorberg Verlag, Suttgart 1996.

3.3. Las posibilidades de un sistema de interceptación que funcione a escala mundial

Hoy en día existen distintos medios de comunicación para la transmisión intercontinental de todo tipo de mensajes (voz, fax y datos). Las posibilidades de un sistema de interceptación que funciones a escala mundial están limitadas por dos factores:

- el acceso limitado al medio de comunicación;
- la necesidad de filtrar una enorme masa de comunicaciones para extraer de ella las comunicaciones interesantes.

3.3.1. El acceso a los medios de comunicación

3.3.1.1. Comunicación por cable

Se transmiten por cable todos los tipos de comunicación (voz, fax, correo electrónico, datos). La comunicación por cable sólo puede interceptarse cuando es posible acceder físicamente al cable. Ello es posible, en cualquier caso, en los extremos de una conexión por cable, cuando el punto de conexión está dentro del territorio del Estado que ordena o permite la interceptación. En el plano interestatal también es posible, **técnicamente hablando**, interceptar los mensajes que circulan por todos los cables, cuando los leyes lo permiten. Sin embargo, los servicios de inteligencia extranjeros no suelen disponer de acceso legal a los cables dentro del territorio de soberanía de otros Estados. Sin embargo, pueden lograr un acceso puntual al cable, de manera ilegal y con un elevado riesgo de ser descubiertos.

Las conexiones intercontinentales por cable se crearon en la época del telégrafo y mediante cables submarinos. Siempre resulta posible acceder a estos cables en los puntos en los que salen del agua. Cuando varios Estados colaboran en la actividad de interceptación se da la posibilidad de acceso a todos los extremos de las conexiones por cable que entran en dichos Estados. Esta circunstancia fue históricamente importante, ya que tanto el cable submarino telegráfico como los primeros cables submarinos coaxiales telefónicos entre Europa y América en Terranova (en territorio de soberanía del Canadá) salían del agua y las comunicaciones con Asia pasaban por Australia, ya que se necesitaban amplificadores intermedios. Hoy en día los cables de fibra óptica se tienden directamente y sin estaciones intermedias en Australia ni en Nueva Zelanda, sin que el relieve escarpado del fondo submarino suponga una dificultad y sin que sean necesarias las instalaciones intermedias de amplificación. Los cables eléctricos también pueden interceptarse entre los extremos de una conexión mediante inducción (es decir, por electromagnetismo, aplicando una bobina al cable), sin crear una conexión eléctrica directa. Esta técnica la emplean, con importante despliegue técnico, los submarinos que detectan comunicaciones transmitidas por cables eléctricos submarinos. Esta técnica la utilizaron los Estados Unidos para "pinchar" un determinado cable submarino de la Unión Soviética por el que se transmitían órdenes no cifradas destinadas a la flota de submarinos nucleares rusa. El empleo generalizado de esta técnica resulta imposible por lo elevado de sus costes.

En el caso de los cables de fibra óptica de la generación anterior utilizados todavía hoy sólo es posible una interceptación inductiva en los amplificadores intermedios. En ellos, la señal óptica se convierte en señal eléctrica; ésta se amplifica y, a su vez, se convierte en señal óptica. No obstante, se plante aquí la cuestión de cómo transportar las enormes cantidades de datos que se

transmiten por un cable de estas características desde el lugar de la interceptación hasta el lugar de la interpretación sin utilizar a su vez un cable propio de fibra óptica. El empleo de un submarino con instalaciones de interpretación a bordo sólo se da en casos muy aislados, por motivos de costes, como, por ejemplo, en situaciones de guerra y para capturar comunicaciones militares estratégicas del enemigo. Para la vigilancia habitual del tráfico telefónico internacional no tiene sentido, a juicio del ponente, emplear un submarino. Los cables de fibra óptica de última generación utilizan un láser de erbio como amplificador intermedio; ello hace imposible el recurso a técnicas electromagnéticas para interceptar los mensajes. Así pues, estos cables de fibra óptica sólo pueden ser interceptados en los extremos de las conexiones.

Aplicado a la práctica, todo ello significa que para el grupo de países que participan en la estructura ECHELON, los **Estados ECHELON**, sólo pueden interceptar a un coste aceptable las comunicaciones transmitidas por cable submarino en los extremos de dicho cable situados en su territorio de soberanía. Así pues, fundamentalmente sólo pueden captar comunicaciones por cable que entran en sus respectivos países o que salen de ellos. Es decir, su acceso a las comunicaciones por cable que entran o salen de sus países se limita, **en Europa**, al **territorio del Reino Unido**.

Hasta ahora, la mayor parte de las comunicaciones internas se transporta por la red nacional de cable; con la privatización de las telecomunicaciones puede haber excepciones, pero éstas son parciales y no predecibles.

Ello es así, por lo menos, por lo que se refiere al teléfono y al telefax; para las comunicaciones por Internet a través de cable, las condiciones son otras. En síntesis, las limitaciones son éstas:

- En Internet, la comunicación se efectúa mediante paquetes de datos; los paquetes dirigidos a un destinatario pueden transitar por distintos caminos dentro de la red.

- En los comienzos de era de Internet, las zonas de menor tráfico dentro de la red científica se aprovechaban para transmitir mensajes electrónicos. Por ello, el camino que iba a seguir un mensaje era completamente impredecible; los paquetes aislados recorrían caminos caóticos imposibles de prever. En aquella época, la conexión internacional más importante era la "red troncal científica" entre Europa y América.

- Con la comercialización de Internet y el establecimiento de proveedores de acceso se produjo una comercialización de la red. Los proveedores de acceso a Internet gestionaban o alquilaban redes propias. Por ello, intentaban cada vez con mayor frecuencia mantener la comunicación dentro de su propia red para evitar pagar derechos de uso a otros miembros de la red. Por esta razón, hoy en día el camino que recorre un paquete de datos dentro de la red no sólo está determinado por la distribución del tráfico, sino que también depende de consideraciones de costes.

- Un mensaje electrónico que el cliente de un proveedor envía al cliente de otro proveedor se mantiene, por regla general, en la red de la empresa, aunque ello signifique que el mensaje no recorre el camino más corto. Los ordenadores que deciden acerca del modo de transporte de los paquetes de datos en los nudos de la red (los denominados "encaminadores") organizan la transición a otras redes en determinados puntos de paso (los denominados "puntos de conmutación")

- En la época de las redes troncales científicas, los puntos de conmutación de la comunicación mundial por Internet estaban situados en los Estados Unidos. Por ello, en aquella época los servicios de inteligencia podían acceder a una parte esencial de la comunicación europea por Internet. Hoy en día, la comunicación intraeuropea por Internet sólo pasa en una proporción muy reducida a través de los Estados Unidos.

- La comunicación intraeuropea pasa en una proporción muy pequeña por un punto de conmutación situado en Londres al que tiene acceso el servicio británico de inteligencia (GCHQ). La mayor parte de las comunicaciones no abandona el continente. Así, por ejemplo, más del 95% de la comunicación alemana por Internet pasa por un punto de conmutación situado en Francfort.

En el terreno práctico, esto significa que los Estados ECHELON sólo tienen acceso a una **parte muy reducida** de la comunicación por Internet a través de cable.

3.3.1.2. Comunicación por ondas[9]

La posibilidad de interceptar comunicaciones transmitidas por ondas depende del alcance de las ondas electromagnéticas empleadas. Si las ondas emitidas se mueven por la superficie terrestre (las denominadas **ondas terrestres**), su alcance es limitado y depende de la estructura del terreno, la presencia de edificios y la vegetación. Si las ondas se proyectan hacia el espacio (las denominadas **ondas indirectas o de espacio**), pueden superar distancias considerables después de reflejarse en capas de la ionosfera. La reflexión múltiple aumenta considerablemente el alcance de la onda.

El alcance de la transmisión depende de la longitud de onda:

- Las ondas largas y muy largas (3kHz-300kHz) sólo se expanden por la onda terrestre, ya que la onda indirecta no se refleja. Tienen un alcance escaso.

- Las ondas medias (300kHz-3MHz) se extienden por la onda terrestre y, de noche, también por la onda indirecta. Tienen alcances medios.

- Las ondas cortas (3MHz-30MHz) se expanden principalmente por la onda indirecta y, por reflexión múltiple, permiten una recepción **de ámbito mundial**.

- Las ondas ultracortas (30MHz-300MHz) sólo se expanden por la onda terrestre, ya que la onda indirecta no se refleja. Se extienden de forma relativamente rectilínea, como la luz, por lo que su alcance depende, por efecto de la curvatura terrestre, de las alturas de las antenas de emisores y receptores. Según su potencia, tienen alcances de 100 km aproximadamente; en el caso de los teléfonos portátiles, su alcance es de unos 30 km.

- Las ondas decimétricas y centimétricas (30MHz-30GHz) se extienden, todavía más que las ondas ultracortas, de forma cuasióptica. Se dejan unir en haces con facilidad y, así, permiten transmisiones dirigidas con precisión y con escasa potencia (tramos terrestres de ondas direccionales). Sólo pueden captarse con una antena cercana, situada en paralelo a

[9] U. Freyer, Nachrichtenübertragungstechnik (Técnica de telecomunicación), Hanser Verlag 2000

la línea de transmisión o dentro de ella o de su prolongación.

Las ondas largas y medias sólo se utilizan para emisoras radiofónicas, radiobalizas, etc. La comunicación militar y civil por radio se efectúa por onda corta y, sobre todo, por onda ultracorta, decimétrica y centimétrica.

De todo lo anterior se desprende que un sistema de interceptación que funcione a escala mundial sólo puede captar comunicaciones transmitidas por onda corta. En todas las otras modalidades de la transmisión radiofónica, la estación de interceptación debe estar, como máximo, a 100 km de distancia (por ejemplo, en un navío o en una embajada).

En la práctica, esto significa que los Estados ECHELON sólo tienen acceso a una parte muy reducida de la comunicación por ondas.

3.3.1.3. Comunicaciones por satélites geoestacionarios de telecomunicaciones[10]

Como se ha mencionado, las ondas decimétricas y centimétricas pueden agruparse en haces con facilidad y en una dirección precisa. Si se lanza una onda direccional hacia un satélite de comunicaciones situado a gran altura en órbita geoestacionaria que recibe la señal, la elabora y vuelve a enviarla a la Tierra, pueden salvarse distancias muy grandes sin emplear cables. El alcance estas transmisiones está limitado solamente, de hecho, por el hecho de que el satélite no pueda recibir señales de cualquier punto de la Tierra ni enviarlas a cualquier punto. Por ello, para garantizar la cobertura global se emplean varios satélites (más detalles, en el Capítulo 4). En principio, si los Estados ECHELON mantienen estaciones de intercepción en las zonas de la Tierra que resultan necesarias, pueden interceptar todo el tráfico telefónico, de fax y de datos canalizado por tales satélites.

3.3.1.4. Las posibilidades de interceptación desde aviones y buques

Se sabe desde hace tiempo que se emplean aviones especiales del tipo AWACS para localizar a otros aviones a gran distancia. El radar de estos aparatos se apoya en un sistema de registro para la identificación de objetivos detectados que puede localizar y clasificar emisiones y establecer una correlación con los contactos de radar. No disponen de capacidad independiente de SIGINT[11]. En cambio, el avión espía EP-3, de vuelo lento, de la Marina de los Estados Unidos posee capacidades de interceptación de microondas y de ondas ultracortas y cortas. Las señales se interpretan directamente a bordo; la aeronave sirve para objetivos puramente militares[12].

Además, también se emplean buques y, cerca de las costas, submarinos para la escucha del tráfico de mensajes de radio militares[13].

3.3.1.5. Las posibilidades de interceptación desde satélites espía

Las ondas de radio se difunden, si no se unen en haces con las antenas correspondientes, en todas

[10] Hans Dodel, Satellitenkommunikation (Comunicación por satélite), Hüthig Verlag 1999.
[11] Carta del Secretario de Estado en el Ministerio de Defensa de la República Federal de Alemania, Sr. Walter Kolbow, de 14.2.2001.
[12] Süddeutsche Zeitung, nº 80, 5.4.2001, p. 6.
[13] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, Nueva York, p. 188 y p. 190.

direcciones; es decir, también en el espacio. Los satélites de inteligencia de señales que orbitan a baja altura pueden captar las señales de las emisoras objeto de observación durante unos pocos minutos cada vez. En zonas densamente pobladas y muy industrializadas, la escucha resulta dificultada por la elevada densidad de emisoras de la misma frecuencia, de forma tal, que apenas es posible seleccionar mediante filtrado las señales individuales[14]. Para la vigilancia continuada de la comunicación civil por ondas radiofónicas, estos satélites no resultan apropiados. Paralelamente, existen satélites SIGINT de los Estados Unidos[15] situados a 42 000 km de altura, en órbita semiestacionaria. A diferencia de los satélites de comunicaciones geoestacionarios, estos satélites tienen una inclinación de 3 a 10 grados, un apogeo de 39 000 a 42 000 km y un perigeo de 30 000 a 33 000 km. Por ello, los satélites no están fijos en órbita, sino que se mueven en una órbita elíptica compleja. Por ello, durante un día cubren una extensión mayor y permiten la localización de fuentes de ondas. Todo ello, junto a las características de los satélites, que por lo demás son de acceso público, indican una utilización puramente militar.

Las señales captadas se transmiten a la estación receptora a través de un enlace descendente en haz de 24 GHz fuertemente concentrado en un punto.

3.3.2. Posibilidades de interpretación automática de comunicaciones interceptadas: el empleo de filtros

Para la escucha de comunicaciones del extranjero no se toma como objetivo una conexión telefónica concreta. Más bien se graba la totalidad o una parte de las comunicaciones transmitidas por los satélites observados o por el cable observado y se filtra mediante ordenadores aplicando palabras clave, ya que la interpretación de todas las comunicaciones captadas resulta absolutamente imposible.

El filtrado de las comunicaciones que pasan por determinadas conexiones es sencillo. Mediante palabras clave pueden aislarse también mensajes de telefax y de correo electrónico. Es posible, incluso, aislar una voz determinada si se adiestra al sistema para reconocerla[16]. En cambio, el reconocimiento automático de palabras pronunciadas por una voz cualquiera resulta hoy en día, a juzgar, por lo menos, por los datos de que dispone el ponente, imposible. Además, las posibilidades de filtrado están limitadas también por otros factores: por la capacidad limitada de los ordenadores, por el problema de las lenguas y, ante todo, por la limitación del número de personas encargadas de leer y evaluar los mensajes filtrados.

Para evaluar las posibilidades de los sistemas de filtro debe tenerse asimismo en cuenta que las posibilidades técnicas plenas de un sistema de escucha que, como éste, se rige por el "principio del aspirador" se distribuyen en distintos temas. Una parte de las palabras clave está relacionada con la seguridad militar; otra parte, con el tráfico de estupefacientes y otras formas de delincuencia internacional; otra procede del mundo del comercio con artículos de doble uso; y otra parte está relacionada con el respeto del embargo. Una parte de las palabras clave también está relacionada con la economía. Esto significa que las capacidades del sistema se dividen en varios ámbitos. Limitar las palabras clave a los ámbitos económicamente interesantes no sólo

[14] Carta del Secretario de Estado en el Ministerio de Defensa de la República Federal de Alemania, Sr. Walter Kolbow, de 14.2.2001.
[15] Mayor Andronov, Zarubezhnoye voyennoye obozreniye (Revista de actualidad militar exterior), nº 12, 1993, pp. 37-43.
[16] Comunicación privada recibida por el ponente; fuente reservada.

estaría en contraposición con las exigencias impuestas a los servicios técnicos por las autoridades políticas, sino que ni siquiera se ha practicado después del final de la Guerra Fría[17].

3.3.3. El ejemplo del Servicio Federal de Inteligencia de la RFA (BND)

La sección 2 del Servicio Federal de Inteligencia alemán (BND) obtiene información mediante la interceptación de comunicaciones del extranjero. Esta actividad fue objeto de examen por el Tribunal Constitucional alemán. Los detalles[18] que se dieron a conocer durante el proceso, junto con las declaraciones del coordinador de los servicios de inteligencia en la Cancillería Federal, Ernst Uhrlau, hechas a la comisión temporal ECHELON el 21 de noviembre de 2000, permiten formarse una idea de las posibilidades de obtención de información que brinda la interceptación de las comunicaciones por satélite.

Es posible que en uno u otro país los servicios de inteligencia dispongan de mayores posibilidades de acción por tener derecho a acceder a las comunicaciones transmitidas por cable o por disponer de más personal encargado de evaluar la información. En particular, en el caso de que se incluyan en la observación los flujos de mensajes transmitidos por cable, la probabilidad estadística de acierto es mayor, pero no lo es necesariamente el número de mensajes aprovechables. De hecho, el ejemplo del Servicio Federal de Inteligencia alemán resulta, a juicio del ponente, especialmente ilustrativo de las posibilidades y estrategias con que cuentan los servicios exteriores de inteligencia para el seguimiento de las comunicaciones en el extranjero, aun cuando no las den a conocer.

El Servicio Federal de Inteligencia alemán intenta conseguir información del extranjero y sobre el extranjero mediante controles **estratégicos** de las telecomunicaciones. Para ello, y con ayuda de una serie de palabras clave de búsqueda (que en Alemania debe aprobar previamente la denominada Comisión G10[19]) se interceptan y evalúan mensajes transmitidos por satélite. Las cifras globales básicas son las siguientes (para el año 2000): de los 10 millones de conexiones de comunicaciones internacionales por día, aproximadamente, que salen y entran en Alemania, 800 000 aproximadamente se efectúan por satélite. De esta proporción, apenas un 10% (75 000) se filtra mediante un dispositivo de búsqueda. Esta limitación no es, a juicio del ponente, consecuencia de la ley (en teoría, antes de la sentencia del Tribunal Constitucional, por lo menos, se habría permitido llegar al 100%), sino consecuencia técnica de otras limitaciones, como por ejemplo de la capacidad limitada de interpretación.

Por otra parte, el número de palabras clave manejables también está limitado por factores técnicos y por las normas de autorización. En la exposición de motivos de la sentencia del Tribunal Federal Constitucional se habla, al margen de claves de búsqueda puramente formales (números de teléfono de extranjeros o de empresas extranjeras en el extranjero), de 2000 palabras clave para el ámbito de la proliferación de armamentos, 1000 para el del comercio de armas, 500 para el del terrorismo y 400 para el del tráfico de estupefacientes. A pesar de ello, en lo tocante al terrorismo y al tráfico de estupefacientes el procedimiento ha dado unos resultados más bien escasos.

[17] Comunicación privada recibida por el ponente; fuente reservada.
[18] Tribunal Federal Constitucional, 1 BvR 2226/94 de 14.7.1999, apartado 1.
[19] Ley de limitación del secreto postal y de las telecomunicaciones (relativa al artículo 10 de la Ley Fundamental) de 13.8.1968.

El dispositivo de búsqueda examina si en los mensajes de telefax y telex aparecen las palabras clave autorizadas. En la actualidad, no es posible el reconocimiento automático de palabras en las comunicaciones de voz. Si los términos clave no aparecen, los mensajes caen automáticamente en la papelera (técnicamente hablando); no pueden ser evaluados ni interpretados, ya que para ello se carece del necesario fundamento jurídico. Cada día se dan aproximadamente cinco casos de comunicaciones de abonados que reciben protección en aplicación de las disposiciones de la Constitución alemana. La labor de investigación estratégica del Servicio Federal de Inteligencia alemán apunta al objetivo de encontrar piezas de un mosaico como elementos en los que apoyarse para sucesivas fases de una investigación. Este servicio no tiene por objetivo, en modo alguno, la vigilancia absoluta de las comunicaciones exteriores. De acuerdo con las informaciones de que dispone el ponente, ello reza también para la actividad SIGINT de otros servicios de inteligencia exterior.

4. La Técnica de las comunicaciones por satélite

4.1. La importancia de los satélites de telecomunicaciones

Hoy, los satélites de telecomunicaciones constituyen un elemento imprescindible de la red mundial de telecomunicaciones, así como del suministro de programas de televisión y radio y servicios multimedia. Sin embargo, la proporción de comunicaciones por satélite en las comunicaciones ha disminuido sustancialmente durante los últimos años en la Europa central. En algunas zonas, ha caído incluso por debajo del 10%[20]. Ello obedece a las ventajas ofrecidas por los cables de fibra óptica, que pueden transmitir un volumen de comunicaciones mucho mayor con una calidad de conexión más alta.

Hoy, las comunicaciones se realizan también en el ámbito vocal por sistemas digitales. La capacidad de las conexiones digitales vía satélite está restringida a **1.890** canales vocales RDSI (64 kbits/s) por transpondedor en el satélite en cuestión. En cambio, hoy en día, una sola fibra óptica puede llevar **241.920** canales vocales con la misma norma. Esto corresponde a un coeficiente de **1:128**.

Además, la calidad de las conexiones vía satélite es más baja que la de las conexiones vía cables de fibra óptica subacuáticos. En el caso de las transmisiones vocales normales, la pérdida de calidad que resulta de los largos períodos de recorrido de las señales -cientos de milisegundos- apenas se nota, aunque es perceptible. En el caso de las comunicaciones de datos y fax, que implican un procedimiento complicado de enlace, el cable ofrece ventajas claras en términos de seguridad de conexión. Al mismo tiempo, sin embargo, solamente el 15% de la población mundial está conectado a la red mundial de cable[21].

Para ciertas aplicaciones, por lo tanto, los sistemas por satélite continuarán ofreciendo a largo plazo ventajas sobre el cable. He aquí algunos ejemplos del ámbito civil:

- Transmisiones nacionales, regionales e internacionales telefónicas y de datos en zonas con un bajo volumen de comunicaciones, es decir, en lugares donde una conexión por cable no sería rentable debido al bajo índice de utilización;

- Sistemas temporales de comunicaciones utilizados en el contexto de intervenciones en caso de catástrofe, acontecimientos importantes, obras de gran envergadura, etc.;

- Misiones de las NU en zonas con una infraestructura de comunicaciones poco desarrollada;

- Comunicaciones empresariales flexibles/móviles que utilizan microestaciones terrestres (VSATS, véase más abajo).

Esta gama amplia de aplicaciones de los satélites en las comunicaciones se explica por las siguientes características: las emisiones de un solo satélite geoestacionario pueden cubrir casi el 50% de la superficie terrestre; las zonas infranqueables ya no representan una barrera. En la zona en cuestión, el 100% de los usuarios están cubiertos tanto en tierra como en el mar o en el aire.

[20] Véase la exposición de motivos de la modificación de la Ley G-10 en Alemania
[21] Página inicial de "Deutsche Telecom": www.detesat.com/deutsch/

Los satélites pueden empezar a funcionar en el plazo de algunos meses, con independencia de la infraestructura disponible sobre el terreno, son más fiables que el cable y pueden sustituirse más fácilmente.

Las siguientes características de las comunicaciones por satélite deben considerarse como inconvenientes: los períodos relativamente largos de recorrido de las señales, la degradación de la propagación, la vida útil más corta (entre 12 y 15 años) en comparación con el cable, la mayor vulnerabilidad y la facilidad de interceptación.

4.2. Cómo funciona un enlace por satélite

Como ya hemos dicho (véase el capítulo 3), utilizando antenas apropiadas las microondas pueden concentrarse fácilmente, permitiendo la sustitución de los cables por haces hertzianos. Si la antena de emisión y de recepción no está en una superficie plana, sino, como en el caso de la tierra, en una superficie esférica, a partir de cierta distancia dada la antena receptora desaparece bajo del horizonte debido a la curvatura de la tierra. Así, las dos antenas ya no se "ven". Esto podría aplicarse también a un enlace intercontinental por haces hertzianos entre Europa y los EE.UU.. Las antenas deberían colocarse en palos de 1,8 km de altura para poder establecer una conexión. Por esta razón, un enlace por haces hertzianos de esta clase no es posible y ello tanto más cuanto que la señal se atenúa en su recorrido por el aire y el vapor de agua. Sí es posible, en cambio, colocar a gran altitud en el espacio y en una posición fija una especie de espejo para los haces hertzianos. Ello permitiría franquear grandes distancias pese a la curvatura de la tierra, de la misma manera que el espejo retrovisor permite ver lo que hay tras una curva. El principio descrito puede aplicarse utilizando satélites geoestacionarios.

4.2.1. Satélites geoestacionarios

Si se coloca un satélite en una órbita circular paralela al ecuador de manera que de la vuelta a la tierra una vez cada 24 horas, el satélite seguirá exactamente la rotación de la tierra. Visto desde la superficie de la tierra, permanecerá inmóvil a una distancia de 36.000 km. Esto significa que tiene una posición geoestacionaria. La mayor parte de los satélites de comunicaciones y de televisión son de este tipo.

4.2.2. La ruta seguida por las señales enviadas vía un enlace de comunicaciones por satélite

La transmisión de señales vía satélite puede describirse como sigue:

La señal que viene de un cable es transmitida por una estación terrestre equipada con una antena parabólica al satélite vía un haz hertziano ascendente llamado "**uplink"**. El satélite recibe la señal, la amplifica y la transmite de nuevo vía un haz hertziano descendiente, el llamado "**downlink"**, hacia otra estación terrestre. Allí, la señal se transfiere de nuevo a una red de cable.

En el caso de las comunicaciones móviles, la señal se transmite directamente de la unidad de comunicación móvil al satélite, desde donde puede introducirse en una conexión por cable, vía una estación terrestre, o retransmitirse directamente a otra unidad móvil.

4.2.3. Sistemas más importantes de comunicación por satélite

Las comunicaciones procedentes de **redes de cable accesibles al público** (que no son necesariamente estatales) se transmiten, en su caso, entre estaciones terrestres fijas vía los sistemas por satélite de distinto alcance, reintroduciéndose después en redes de cable. Se puede distinguir entre los sistemas por satélite siguientes:

- sistemas globales (por ejemplo la INTELSAT)

- sistemas por zonas (continentales) (por ejemplo EUTELSAT)

- sistemas nacionales (por ejemplo ITALSAT).

La mayoría de estos satélites están en una órbita geoestacionaria; 120 empresas privadas explotan unos 1.000 satélites[22] en todo el mundo.

Además, las zonas muy septentrionales de la tierra están cubiertas por satélites en una órbita especialmente excéntrica (órbitas rusas Molnyia), que son visibles para usuarios de estas zonas en la mitad de su órbita. Dos satélites pueden proporcionar una cobertura regional completa, que no es posible desde una posición geoestacionaria por encima del ecuador.

Por otra parte, INMARSAT, un sistema global establecido originalmente para su uso en alta mar, proporciona un **sistema de comunicaciones móviles** mediante el cual se pueden crear enlaces por satélite en cualquier lugar del mundo. Este sistema utiliza también satélites geoestacionarios.

El sistema de comunicaciones por satélite basado en la telefonía móvil IRIDIUM, que empleaba satélites colocados en órbitas bajas diferidas, dejó de funcionar recientemente por razones económicas (nivel de utilización insuficiente).

Hay también un mercado en rápida expansión para las llamadas conexiones VSAT (VSAT = terminal de abertura muy pequeña). Se trata de microestaciones terrestres con un diámetro de entre 0,9 y 3,7 metros, explotadas por empresas para cubrir sus propias necesidades (por ejemplo las videoconferencias) o por prestatarios de servicios móviles para demandas de comunicaciones temporales (por ejemplo, reuniones). En 1996, funcionaban en todo el mundo 200.000 microestaciones terrestres. Volkswagen AG explota 3.000 unidades VSAT, Renault 4.000, la General Motors 100.000 y la mayor empresa petrolera europea 12.000. La comunicación es totalmente abierta, a menos que el cliente la codifique por su cuenta[23].

4.2.3.1. Sistemas mundiales de comunicaciones por satélite

Estos sistemas por satélite cubren todo el globo gracias a la colocación de satélites en las zonas del Atlántico, del Índico y del Pacífico.

INTELSAT[24]

[22] G. Thaller, Satelliten im Erdorbit, Franzisverlag, Munich, 1999.
[23] H. Dodel, declaración hecha en privado.
[24] INTELSAT-página inicial http:/www.intelsat.com.

La INTELSAT (Organización Internacional de Telecomunicaciones por Satélite), que se fundó en 1964, es una autoridad con una estructura organizativa similar a la de las NU y con el propósito comercial de proporcionar comunicaciones internacionales. Los miembros de la organización eran empresas de propiedad estatal de telecomunicaciones. Hoy, 144 gobiernos son miembros de la INTELSAT. La INTELSAT se privatizará en 2001 .

Actualmente, la INTELSAT gestiona una flota de 19 satélites geoestacionarios que proporcionan conexiones entre más de 200 países. Los servicios de la INTELSAT se alquilan a sus miembros. Los miembros explotan sus propias estaciones terrestres. Gracias al servicio comercial de la INTELSAT (IBS), los no miembros (por ejemplo las empresas telefónicas, las grandes empresas y las empresas multinacionales) pueden utilizar también los satélites. La INTELSAT ofrece servicios globales tales como comunicaciones, televisión, etc. Las telecomunicaciones se efectúan en bandas C y Ku (véase más abajo).

Los satélites de la INTELSAT son los satélites internacionales más importantes en el ámbito de las telecomunicaciones. A través de ellos se efectúa la mayor parte de las comunicaciones internacionales por satélite.

Los satélites cubren las zonas del Atlántico, del Indico y del Pacífico (véase el cuadro del capítulo 5,5.3).

Existen diez satélites sobre el Atlántico entre 304ºE y 359ºE, la zona del Índico está cubierta por seis satélites situados entre 62ºE y 110,5ºE y la zona del Pacífico por tres satélites situados entre 174ºE y 180ºE. El gran volumen de comunicaciones en la región atlántica lo cubren varios satélites individuales.

INTERSPUTNIK[25]

La organización internacional de comunicaciones por satélite INTERSPUTNIK fue fundada en 1971 por nueve países como una agencia de la antigua Unión Soviética con una misión similar a la de la INTELSAT. Hoy, INTERSPUTNIK es una organización intergubernamental a la que puede adherirse el gobierno de cualquier país. Actualmente, tiene 24 miembros (incluida Alemania) y unos 40 usuarios (incluidas Francia e Inglaterra), representados por sus administraciones postales o empresas nacionales de telecomunicaciones. Su sede está en Moscú.

Las telecomunicaciones se transmiten por las bandas C y Ku (véase más abajo).

Sus satélites (Gorizont, Express y Express A, de la Federación Rusa, y LMI-1, de la empresa mixta Lockheed-Martin) cubren también todo el globo: hay un satélite en la zona atlántica, se prevé colocar otro la zona del Índico y existen dos más en la zona del Pacífico (véase el cuadro del capítulo 5,5.3).

INMARSAT

Desde 1979 INMARSAT (Interim International Maritime Satellite) ha proporcionado, mediante su sistema por satélite, comunicaciones móviles a nivel internacional en alta mar, en el aire y en tierra, así como un sistema de radio de urgencia. INMARSAT se creó a iniciativa de la

[25] Página inicial de INTERSUTNIK: http://www.intersputnik.com

Organización Marítima Mundial como organización internacional. INMARSAT se ha privatizado y tiene su sede en Londres.

El sistema INMARSAT consiste en nueve satélites en órbitas geoestacionarias. Cuatro de estos satélites - la tercera generación de INMARSAT - cubren todo el globo a excepción de las zonas polares extremas. Cada satélite cubre aproximadamente una tercera parte de la superficie terrestre. Su situación sobre las cuatro regiones oceánicas (Atlántico occidental y oriental, Pacífico y Océano Índico), permite una cobertura global. Al mismo tiempo, cada INMARSAT tiene varios sub-haces ("spot beams") que permiten concentrar la energía en las zonas con un mayor volumen de comunicaciones.

Las telecomunicaciones se efectúan por las bandas L y Ku (véase más abajo).

4.2.3.2. Sistemas por satélite regionales

Las zonas de emisión de los sistemas por satélite regionales cubren regiones y continentes individuales. Por consiguiente, las comunicaciones que se transmiten vía estos sistemas pueden recibirse solamente en esas regiones.

EUTELSAT[26]

EUTELSAT la fundaron en 1977 17 administraciones de correos europeas con el objetivo de cubrir las necesidades de comunicación por satélite propias de Europa y de apoyar a la industria espacial europea. Tiene su sede en París y unos 40 países miembros. Está previsto privatizar EUTELSAT en 2001.

EUTELSAT gestiona 18 satélites geoestacionarios que cubren Europa, África y amplias partes de Asia y establecen un vínculo con América. Los satélites están situados entre 12.5ºO y 48ºE. EUTELSAT ofrece básicamente servicios de televisión (850 canales digitales y analógicos) y radio (520 canales), pero proporciona también enlaces de comunicaciones, sobre todo en Europa, incluida Rusia, por ejemplo para videoconferencias, para redes privadas de grandes empresas (entre otras, la General Motors y Fiat), para agencias de prensa (Reuters, AFP), para los proveedores de información financiera y para los servicios móviles de transmisión de datos.

Las telecomunicaciones se transmiten por la banda Ku.

ARABSAT[27]

ARABSAT es el equivalente de EUTELSAT en la zona árabe y se fundó en 1976. La integran 21 países árabes. Los satélites de ARABSAT se utilizan tanto para la transmisión de servicios de televisión como para las comunicaciones.

Las telecomunicaciones se transmiten principalmente por la banda C.

PALAPA[28]

[26] Página inicial de EUTELSAT: http://www.com.
[27] Página inicial de ARABSAT: http://www.arabsat.
[28] H. Dodel, Satellintenkommunication, Hüthigverlag 1999.

El sistema indonesio PALAPA funciona desde 1995 y es el equivalente de EUTELSAT en el Asia meridional. Sus emisiones cubren Malasia, China, el Japón, la India, Pakistán y otros países de la zona.

Las telecomunicaciones se realizan por las bandas C y Ku.

4.2.3.3. Sistemas por satélite nacionales[29]

Muchos Estados cubren sus propias necesidades explotando sistemas por satélite con huellas restringidas.

El satélite de telecomunicaciones francés **TELECOM** sirve, entre otras cosas, para conectar a los departamentos franceses en África y Sudamérica a Francia. Las telecomunicaciones se realizan por las bandas C y Ku.

ITALSAT explota los satélites de telecomunicaciones que cubren el conjunto de Italia mediante huellas contiguas. Así pues, la recepción sólo es posible en Italia. Las telecomunicaciones se realizan por la banda Ku.

AMOS es un satélite israelí que ofrece básicamente servicios de comunicación en lugares fijos y su huella cubre el Oriente Próximo. Las telecomunicaciones se transmiten por la banda Ku.

Los satélites españoles **HISPASAT** cubren España y Portugal (puntos de Ku) y transmiten programas españoles de televisión a América del Norte y América del Sur.

4.2.4. La asignación de frecuencias

La Unión internacional de telecomunicaciones es responsable de la asignación de frecuencias. Para facilitar la organización, se dividió el mundo en tres zonas, a efectos de comunicación por radio:

1. Europa, África, antigua Unión Soviética y Mongolia

2. América del Norte, América del Sur y Groenlandia

3. Asia, excepto los países de la zona 1, Australia y el Pacífico Sur.

Esta división histórica se adoptó para las comunicaciones por satélite y ha dado lugar a la acumulación de satélites en ciertas zonas geoestacionarias. Las bandas de frecuencia más importantes para las comunicaciones por satélite son:
- La banda L (0,4 - 1,6 GHz) para comunicaciones por satélite móviles, por ejemplo vía IMMARSAT;

- La banda C (3,6 - 6,6 GHz) para las estaciones terrestres, por ejemplo vía INTELSAT;

- La banda Ku (10 - 20 GHz) para las estaciones terrestres, por ejemplo punto Ku de INTELSAT y EUTELSAT;

[29] H. Dodel e investigaciones internas.

- La banda Ka (20 - 46 GHz) para las estaciones terrestres, por ejemplo vía satélites nacionales tales como ITALSAT;

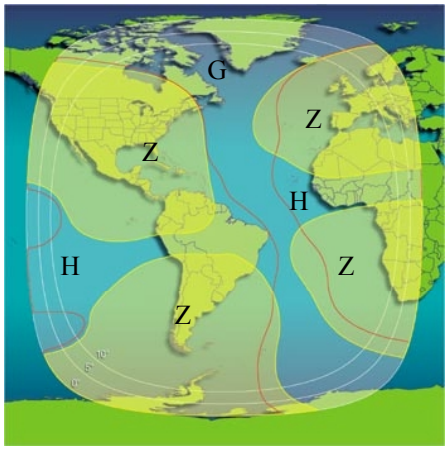
- La banda V(46 - 56 GHz) para las microestaciones terrestres (VSAT).

4.2.5. Huellas de los satélites (footprints)

La huella es la zona de la tierra cubierta por una antena de satélite. Puede abarcar hasta el 50% de la superficie de terrestre o, cuando la señal se concentra, puntos regionales más pequeños.

Cuanto más alta es la frecuencia de la señal emitida, mayores son las posibilidades de concentración de la misma y, por consiguiente, de reducción de la huella. La concentración de la señal emitida por el satélite en huellas menores puede aumentar la energía de la señal. Cuanto menor sea la huella, más fuerte puede ser la señal, por lo que las antenas de recepción pueden ser también menores.

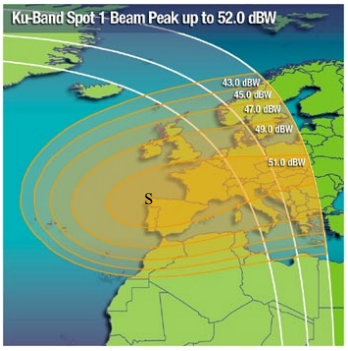
Para los satélites INTELSAT, la situación se puede resumir más detalladamente como sigue:

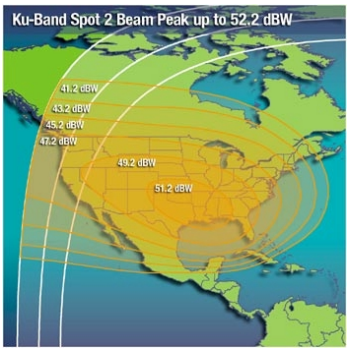


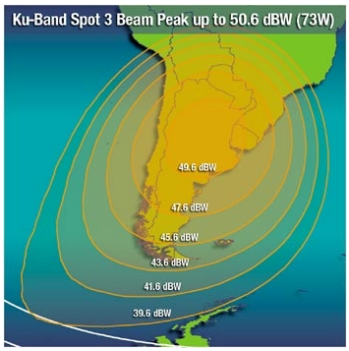
Las huellas de los satélites de INTELSAT se dividen en distintos haces:

El haz global de los satélites (G) cubre aproximadamente una tercera parte de la superficie de terrestre;

Los haces hemisféricos (H) cubren una zona ligeramente inferior a la mitad de la zona cubierta por los haces globales. Los haces zonales (Z) son puntos en zonas particulares de la tierra; son más pequeños que los haces hemisféricos. Además existen los llamados sub-haces: éstas son huellas precisas y reducidas (véase más abajo).







Los haces globales, hemisféricos y de zona utilizan frecuencias de la banda C. Los sub-haces utilizan frecuencias de la banda Ku.

4.2.6. El tamaño de las antenas requerido para una estación terrestre

Las antenas de recepción terrestres son antenas parabólicas. El espejo parabólico refleja todas las

ondas captadas y las concentra en un punto focal. El sistema de recepción real está situado en el foco del espejo parabólico. Cuanto mayor es la energía de la señal en el punto de recepción, más pequeño puede ser el diámetro de la antena parabólica.

Para el propósito de la investigación llevada a cabo para este informe es esencial que parte de las comunicaciones intercontinentales se transmite por la banda C en los haces globales de los satélites de la INTELSAT y otros (por ejemplo INTERSPUTNIK) y que para su recepción se necesitan platos de satélite con un diámetro de aproximadamente 30 m (véase el capítulo 5). Las antenas de 30 m eran también necesarias para las primeras estaciones creadas para interceptar comunicaciones por satélite, puesto que la primera generación de satélites de la INTELSAT tenía solamente haces globales y la tecnología de transmisión de señal era mucho menos sofisticada que hoy. Estos platos, algunos de los cuales tienen un diámetro de más de 30 m, aún se utilizan en las estaciones en cuestión, aunque ya no sean técnicamente necesarios.

Hoy, las antenas típicas requeridas para las comunicaciones de INTELSAT en la banda C tienen un diámetro entre de 13 y 18 m. En algunos casos concretos, por ejemplo INTELSAT 511, se requiere una antena más grande para el haz global. En el caso de los satélites más nuevos de INTELSAT, son suficientes antenas con un diámetro de hasta 5 m para los haces zonales en la banda C.

Para recibir comunicaciones en la banda C de INTERSPUTNIK se necesitan antenas con un diámetro de entre 2 y 25 m.

Para los puntos de Ku de los satélites de INTELSAT y otros (banda Ku de EUTELSAT, banda Ku de AMOS, etc.) se requieren antenas con un diámetro entre de 2 y 10 m .

En el caso de las microestaciones terrestres, que funcionan en la banda V y cuya señal, en virtud de la alta frecuencia, puede concentrarse en mayor medida que en la banda Ku, son suficientes antenas con un diámetro entre de 0,9 y 3,7 m (por ejemplo VSAT de EUTELSAT o de INMARSAT).

5. Pruebas consistentes en indicios de la existencia de por lo menos un sistema mundial de interceptación

5.1. ¿Por qué son necesarias pruebas consistentes en indicios?

Los servicios secretos no revelan detalles acerca de su trabajo. Por lo tanto no existe ninguna declaración oficial de los servicios de inteligencia exterior de los Estados de ECHELON en la que se afirme que gestionan conjuntamente un sistema mundial de interceptación. Así pues, hay que demostrar la existencia de este sistema buscando tantos indicios como sea posible, a fin de desarrollar un cuerpo convincente de pruebas.

La cadena de indicios que constituyen una prueba está compuesta por tres elementos:

- Pruebas de que los servicios de inteligencia exterior de los Estados ECHELON interceptan comunicaciones privadas y de las empresas;
- Pruebas de que se pueden encontrar estaciones de interceptación gestionadas por ECHELON en las partes de la tierra donde son necesarias debido a los requisitos técnicos del sistema civil de comunicación por satélite;
- Pruebas de que, entre los servicios de inteligencia de estos Estados, existe una asociación más estrecha de lo habitual. Que esta cooperación vaya hasta la aceptación por los socios de contratos de interceptación y la comunicación directa por éstos del material bruto interceptado, sin explotación propia, es irrelevante para demostrar que existe una asociación. Ello no tiene ninguna importancia a la hora de saber cuál es la jerarquía en esta asociación.

5.1.1. Pruebas de la actividad de interceptación por parte de servicios de inteligencia exterior

Por lo menos en las democracias, los servicios de inteligencia funcionan sobre la base de las leyes que definen su propósito y/o poderes. Así, es fácil probar que en muchos de estos países existen servicios de inteligencia exterior que interceptan comunicaciones civiles. Esto es cierto también para los cinco Estados ECHELON, que utilizan estos servicios. No se necesita ninguna prueba adicional específica de que cualquiera de estos Estados intercepta las comunicaciones que entran y salen de su territorio. Desde el propio territorio puede captarse también, mediante satélites de comunicaciones, una parte de los mensajes cuyos destinatarios se encuentran en el extranjero. En ninguno de los cinco Estados de ECHELON existen limitaciones jurídicas que impidan a los servicios de inteligencia actuar de esta manera. La lógica interna del método de control estratégico de las comunicaciones exteriores y el objetivo de este control, conocido al menos en parte, hacen pensar que es así como actúan.

5.1.2. Pruebas de la existencia de estaciones en las zonas geográficas necesarias

La única limitación al intento de desarrollar la supervisión de las comunicaciones por satélite en todo el mundo la plantean las restricciones técnicas impuestas por las comunicaciones mismas. No hay ningún lugar desde el que puedan interceptarse **todas** las comunicaciones por satélite (véase el capítulo 4, 4.2.5).

Sería posible desarrollar un sistema de interceptación a escala internacional con tres condiciones:
- el operador tiene una parte de su territorio nacional en todas las partes necesarias del mundo;
- el operador tiene, en todas las partes necesarias del mundo, una parte de su territorio nacional o un derecho de acceso en las partes restantes del mundo o puede gestionar en ellas estaciones o ejercer un derecho de utilización compartida de las mismas;
- el operador es un grupo de Estados que ha formado una asociación de inteligencia y gestiona el sistema en las partes necesarias del mundo.

Ninguno de los Estados de ECHELON podría gestionar un sistema mundial por su cuenta. Los EE.UU. no tienen, por lo menos oficialmente, ninguna colonia. Canadá, Australia y Nueva Zelanda no tienen ninguna parte del territorio nacional fuera del país en sentido estricto y el Reino Unido tampoco podría gestionar por sí solo un sistema global de interceptación (véase el capítulo 6).

5.1.3. Pruebas de una asociación estrecha entre servicios de inteligencia

Por otra parte no se ha revelado si y hasta qué punto los Estados de ECHELON cooperan entre sí en el ámbito de la inteligencia. Normalmente, la cooperación entre servicios de inteligencia es bilateral y se basa en el intercambio de material evaluado. La cooperación multilateral es muy poco corriente; si a ello añadiéramos el intercambio regular de material bruto, estaríamos en presencia de un fenómeno totalmente nuevo. La existencia de una cooperación de este tipo sólo puede probarse sobre la base de indicios.

5.2. ¿Cómo reconocer una estación de interceptación de comunicaciones por satélite?

5.2.1. Criterio 1: accesibilidad de la instalación

Las instalaciones de los servicios de correos, de la radiotelevisión o de las instituciones de investigación, que están provistas de antenas grandes, son accesibles a los visitantes, por lo menos previo aviso; las estaciones de interceptación, en cambio, no lo son. Generalmente su gestión corre a cargo de militares, que llevan también a cabo el trabajo técnico de interceptación. En el caso de la NSA, por ejemplo, las estaciones las gestiona el Grupo de seguridad naval (NAVSECGRU) o la Agencia de inteligencia del aire de las fuerzas aéreas de los EE.UU. (AIA). En las estaciones británicas, la Royal Air Force gestiona las instalaciones para el servicio de inteligencia británico (GCHQ). Ello permite un control militar estricto de las instalaciones, así como el camuflaje de sus actividades.

5.2.2. Criterio 2: el tipo de antena

En las instalaciones que cumplen el criterio 1, se utilizan distintos tipos de antenas, cada uno con una forma distinta que proporciona información en cuanto al propósito de la estación de interceptación. Así, los conjuntos de antenas verticales que forman un círculo de gran diámetro (antenas Wullenweber) se utilizan para averiguar la orientación de las señales de radio. Los conjuntos circulares de antenas romboidales (antenas "pusher") responden al mismo propósito. Las antenas de recepción multidireccionales o direccionales que parecen antenas clásicas de TV gigantescas, se utilizan para interceptar señales de radio no dirigidas. Sin embargo, para recibir

señales de satélites se utilizan sólo antenas parabólicas. Si las antenas parabólicas se colocan en un sitio abierto, es posible calcular, sobre la base de su posición, su ángulo de inclinación (elevación) y su orientación (acimut), qué satélite se está recibiendo. Esto es posible, por ejemplo, en Morwenstow (Reino Unido), Yakima (EE.UU.) y Sugar Grove (EE.UU.). Sin embargo, las antenas parabólicas se ocultan a menudo bajo cubiertas blancas esféricas conocidas como cúpulas: estas cúpulas protegen a las antenas, pero sirven también para ocultar su orientación.

Si se encuentran antenas o cúpulas en el terreno de una estación de interceptación, es seguro que reciben señales de satélites, aunque no se puede saber qué tipo de señales.

5.2.3. Criterio 3: tamaño de la antena

Las antenas receptoras situadas en instalaciones que cumplen el criterio 1 puede estar destinadas a distintos fines:

- estación receptora para comunicaciones militares;
- estación receptora para satélites espía (fotos, radar);
- estación receptora para satélites militares SIGINT;
- estación receptora para la interceptación de satélites de comunicaciones civiles.

Desde el exterior no se puede saber para qué sirven las antenas o cúpulas. Sin embargo, hay tamaños mínimos, dictados por requisitos técnicos, para antenas destinadas a recibir el haz global en la banda C de las comunicaciones internacionales civiles por satélite. La primera generación de estos satélites requería antenas con un diámetro de 25-30 m; hoy en día 15-18 m son suficientes. El filtrado automático de las señales captadas por ordenador requiere una calidad óptima de la señal. Así, cuando lo que se pretende es obtener información, se opta por una antena de dimensiones máximas. Como las antenas están montadas en soportes, el diámetro de las cúpulas es aún mayor que el de las antenas.

5.2.4. Conclusión

Por lo que sabe este ponente, no existe ninguna aplicación militar para antenas de este tamaño. Si se detecta su presencia en un terreno del criterio 1, esto significa que se interceptan comunicaciones civiles por satélite.

5.3. Datos de dominio público sobre estaciones de interceptación conocidas

5.3.1. Método

Para examinar las estaciones que cumplen los criterios recogidos en el punto 5.2. y que forman parte del sistema mundial de interceptación, así como sus labores, se procedió al examen de la literatura existente en la materia, en ocasiones contradictoria (Hager[31], Richelson[32], Campbell[33]),

[31] HAGER, NICKY: Exposing the global surveillance system, http://www.ncoic.com/echelon1.htm
HAGER, NICKY: Secret Power. New Zealands´s Role in the international Spy Network, Nueva Zelanda,1996
[32] RICHELSON, JEFFREY, Desperately seeking Signals, 4 2000, The Bulletin of the Atomic Scientists,

de documentos desclasificados[34], de la página web de la Federación de Científicos de los Estados Unidos[35] y de las de distintos operadores[36] (NSA, AIA, etc.), así como de otras publicaciones en Internet. Además, se han agrupado las huellas de los satélites de comunicación, se han calculado las dimensiones necesarias de las antenas y se han incluido en mapas mundi con las posibles estaciones.

5.3.2. Análisis concreto

Para el examen, se aplican los principios relacionados con la física de la comunicación por satélite que figuran a continuación (véase igualmente el capítulo 4):

- Una antena de satélite únicamente puede captar lo que se encuentra dentro de su huella. Para poder recibir comunicaciones que se realizan principalmente en las bandas C y Ku, la antena debe situarse dentro de las huellas que contienen las bandas C y Ku.
- Para cada haz global es necesaria una antena de satélite, incluso en aquellos casos en que se solapen los haces de dos satélites.
- En caso de que un satélite tenga más huellas que el haz global, tal y como es el caso de la generación de satélites presente, con una sola antena no se pueden captar todas las comunicaciones que se transmiten a través de ese satélite, ya que una única antena no puede estar en todas las huellas. Por lo tanto, para captar los haces hemisféricos y globales de un satélite son necesarias dos antenas situadas en distintos lugares (véase la descripción de las huellas en el capítulo 4). En caso de que haya más haces ("haces zonales y sub-haces"), serían necesarias más antenas. Una antena puede captar distintos haces que se solapen, ya que, técnicamente, las distintas bandas de frecuencia se pueden separar en el momento de la recepción.

Además, se aplican las disposiciones recogidas en el punto 5.2.: la no accesibilidad a las instalaciones, ya que están gestionadas por militares,[37] la necesidad de utilizar antenas parabólicas para la recepción de señales por satélite, y que el tamaño de las antenas de satélite para captar la banda C en el haz global se sitúa en más de 25 m. en el caso de la primera generación INTELSAT y que debe oscilar entre los 15 y los 18 metros en lo que se refiere a las generaciones siguientes.

5.3.2.1. Paralelismo entre el desarrollo de INTELSAT y la construcción de estaciones

---

http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
RICHELSON,T.JEFFREY, The U.S. Intelligence Community, Westview Press,1999

[33] CAMPBELL, DUNCAN, Development of Surveillance Technology and Risk of Abuse of Economic Information, vol. 2/5, 10 1999, STOA, http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
CAMPBELL, DUNCAN: Inside Echelon, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
CAMPBELL, DUNCAN: Interception Capabilities n- Impact and Exploitation – Echelon and its role in COMINT, presentado a la Comisión ECHELON del Parlamento Europeo el 22 de enero de 2001.
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html

[34] RICHELSON, JEFFREY: Newly released documents on the restrictions NSA places on reporting the identities of US-persons: Declassified: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[35] Federation of American Scientists

[36] Military.com; *.mil-Homepages

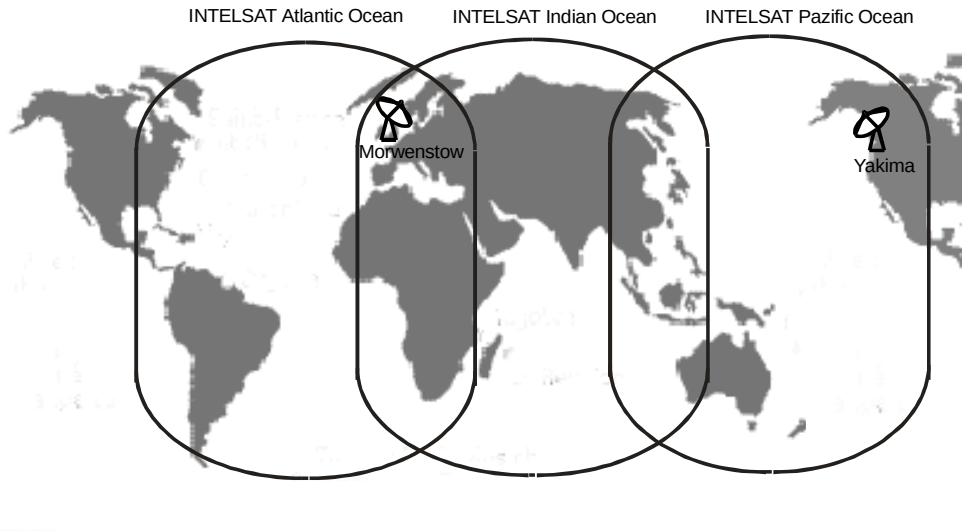
[37]Abreviaturas utilizadas: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Sqadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

Todo sistema de interceptación mundial debe tener en cuenta los avances en el ámbito de las comunicaciones. El inicio de las comunicaciones por satélite implica, necesariamente, la creación de estaciones, y las nuevas generaciones de satélites implican la creación de nuevas estaciones y la construcción de nuevas antenas de satélite que cumplan los requisitos necesarios. El número de estaciones y de antenas de satélite debe aumentar en función de las necesidades de interceptación de las comunicaciones.
Por el contrario, si en las nuevas huellas surgen nuevas estaciones y se construyen nuevas antenas de satélite, no se trata de ninguna casualidad sino que puede considerarse la prueba de la existencia de una estación de interceptación de comunicaciones.
Teniendo en cuenta que los satélites INTELSAT fueron los primeros satélites de comunicaciones que, además, cubrieron todo el planeta, es lógico que la creación y la ampliación de las estaciones sea paralela al desarrollo de las generaciones de satélites INTELSAT.

La primera generación

El primer satélite INTELSAT (Early Bird) ya fue colocado en órbita geoestacionaria en 1965. Por aquel entonces, su capacidad de transmisión aún era reducida y su huella sólo se extendía por el hemisferio norte.
Las generaciones INTELSAT II y III, que comenzaron a ser explotadas en 1967 y 1968, permitieron alcanzar, por primera vez, una cobertura mundial. Los haces globales de los satélites cubrían las zonas del Atlántico, Pacífico e Índico. Por aquel entonces todavía no había huellas de menores dimensiones. Para captar todas las comunicaciones eran necesarias, por lo tanto, tres antenas de satélite. Teniendo en cuenta que dos de los haces globales se solapaban sobre el espacio europeo, en este territorio se podían captar las huellas mundiales de dos satélites con una estación que tuviese dos antenas de satélite con diferente orientación.

Primera generación de satélites INTELSAT de cobertura mundial



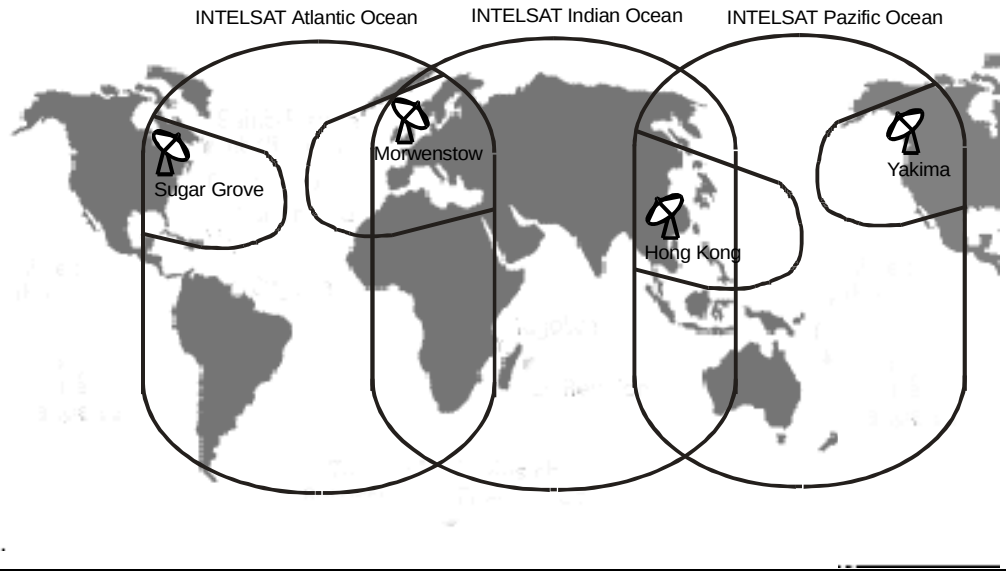
En 1970, se abrió **Yakima**, en el noroeste de los Estados Unidos y en 1972/73, **Morwenstow**, en el Sur de Inglaterra. Yakima contaba entonces con una antena de grandes dimensiones (orientada hacia el Pacífico) y Morwenstow tenía dos antenas de grandes dimensiones (una orientada hacia el Atlántico y otra hacia el Océano Índico). La localización de estas dos estaciones permitía captar la totalidad de las comunicaciones. En 1974 de construyó la primera antena de satélite de

grandes dimensiones en Menwith Hill.

La segunda generación mundial

En los años 70 (1971 e 1975) se desarrolló y se puso en órbita geoestacionaria la segunda generación de satélites INTELSAT (IV y IVA). Los nuevos satélites, que también garantizaban una cobertura mundial y disponían de un número claramente mayor de canales (4000 a 6000), tenían también haces zonales en el hemisferio norte, además de haces globales (véase el capítulo 4). Un haz zonal cubría las regiones orientales de los EE.UU., otro las occidentales, un tercero la Europa Occidental y un cuarto el Asia Oriental. Por lo tanto, en aquel entonces dos estaciones con tres antenas de satélites ya no podían interceptar todas las comunicaciones. Las estaciones existentes en Yakima permitían cubrir el haz zonal de las regiones occidentales de los EE.UU., y, Morwenstow, el haz zonal de Europa. Para captar los otros dos fue necesario establecer una estación en el Oeste de los EE.UU. y otra en la región del Asia Oriental.

Segunda generación de satélites INTELSAT de cobertura mundial



A finales de los años 70 se construyó la estación de **Sugar Grove** en las región oriental de los EE.UU. (la estación ya se utilizaba para interceptar comunicaciones rusas), que entró en funcionamiento en 1980. También a finales de los años 70 se creó una estación en **Hong Kong** . De este modo, en los años 80 había una interceptación mundial de las comunicaciones vía INTELSAT basada en estas cuatro estaciones (Yakima, Morwenstow, Sugar Grove y HongKong).

Los satélites INTELSAT posteriores, con haces zonales y sub-haces además de los globales y de los hemisféricos impulsaron la apertura de otras estaciones en distintas regiones del mundo. En este caso resulta muy difícil establecer una relación entre la creación de nuevas estaciones y la instalación de nuevas antenas de satélites.

Teniendo en cuenta, además, que es muy difícil obtener informaciones sobre las estaciones, no se puede determinar exactamente cuáles son los satélites que se pueden captar desde cada estación

y con qué haz. Sin embargo, se puede determinar en que haz se encuentran las estaciones conocidas.

5.3.2.2. Cobertura mundial por estaciones que interceptan, sin duda alguna, los satélites de comunicaciones

La comunicación mundial por satélite la garantizan en la actualidad los satélites de INTELSAT, INMARSAT e INTERSPUTNIK. Al igual que con las primeras generaciones de satélites, se ha mantenido la división en tres huellas (las zonas del Índico, del Atlántico y del Pacífico). En cada una de las huellas se encuentran estaciones a las que se aplican los criterios característicos de las estaciones de interceptación:

Satélites sobre el Océano Índico :

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT zona del Índico	Geraldton, Australia Pine Gap, Australia Morwenstow, Reino Unido Menwith Hill, Reino Unido
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australia Pine Gap, Australia Misawa, Japón

Satélites sobre el Océano Pacífico :

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT zona del Pacífico	Waihopai, Nueva Zelanda Geraldton, Australia Pine Gap, Australia Misawa, Japón Yakima, EE.UU. - sólo Intelsat e Inmarsat

Satélites sobre el Océano Atlántico:

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°W), 3A (11°W) INMARSAT zona del Atlántico	Sugar Grove, EE.UU. Buckley Field, EE.UU Sábana Seca, Puerto Rico Morwenstow, Reino Unido Menwith Hill, Reino Unido
INTELSAT 707 (359°)	Morwenstow, Reino Unido Menwith Hill, Reino Unido

De este modo se demuestra que es posible un sistema mundial de interceptación de las comunicaciones.

Además, hay otras estaciones a las que no se puede aplicar el criterio relativo a las dimensiones de las antenas que, no obstante, pueden formar parte del sistema mundial de interceptación. Con estas estaciones se podrían captar, por ejemplo, los haces zonales o sub-haces de los satélites cuyos haces globales son interceptadas por otras estaciones o para cuyo haz global no es necesaria una antena de satélite de grandes dimensiones.

5.3.2.3. Descripción detallada de las estaciones

En la descripción detallada de las estaciones se hace una diferenciación entre las estaciones que no hay duda que interceptan satélites de comunicaciones (criterios recogidos en el apartado 5.2.) y las estaciones cuya misión no puede indicarse sobre la base de los criterios señalados anteriormente.

5.3.2.3.1. Estaciones de interceptación de satélites de comunicación

Los criterios recogidos en el punto 5.2., que pueden definirse como indicios de la existencia de una estación de interceptación de las comunicaciones por satélite, se aplican a las siguientes estaciones:

Yakima, EE.UU. (120°O, 46°N)

Estación creada en 1970 conjuntamente con la primera generación de satélites. Desde 1995 se encuentra en ella el 544º Grupo de Inteligencia (Destacamento 4) de la Air Intelligence Agency, Agencia de Inteligencia del Aire, AIA. También está estacionado en esta base el Naval Security Group (NAVSECGRU). Esta estación cuenta con seis antenas de satélite. Nuestras fuentes no facilitan ningún tipo de información sobre su tamaño. Hager las describe como grandes y señala que están orientadas hacia los satélites Intelsat sobre el Pacífico (2 antenas de satélite) y los satélites Intelsat sobre el Atlántico, así como hacia el satélite Immarsat 2.
La fecha de creación de Yakima, que coincide con la primera generación de satélites Intelsat, así como las misiones del 544º Grupo de inteligencia, apuntan a que Yakima desempeña un papel en la interceptación mundial de las comunicaciones. Otro indicio en este sentido es la proximidad de Yakima a una estación de interceptación por satélite, situada a mil millas hacia el norte.

Sugar Grove, EE.UU. (80°O, 39°N)

Sugar Grove se creó simultáneamente con la entrada en funcionamiento de la segunda generación de satélites Intelsat a finales de los años 70. En esta base están estacionados el NAVSECGRU, y la AIA con el 544º Grupo de Inteligencia (Destacamento 3). Según las informaciones de distintos autores, la estación cuenta con 10 antenas de satélite, de las cuales 3 tienen un tamaño superior a los 18 metros (18,2 m, 32,3 m, y 46 m) por lo que no hay duda de que se dedican a la interceptación de las comunicaciones por satélite. Una de las misiones del Destacamento 3 del 544º GI estacionado aquí es brindar ayuda en el ámbito de la información ("Intelligence Support") para recabar información sobre los satélites de comunicaciones a través de las estaciones de la Marina.[38]
Además, Sugar Grove está situada en las proximidades de la estación de interceptación de satélites de Etam (a 60 millas de distancia) .

Sábana Seca, Porto Rico (66°W, 18°N)

El NAVSECGRU se estacionó en 1952 en Sábana Seca. Desde 1995, también se encuentra ahí la AIA con el 544° GI (Destacamento 2). La estación cuenta, como mínimo con una antena de satélite de 32 metros de diámetro y con otras antenas de satélite de menor tamaño.
Según informaciones oficiales, la misión de esta estación es el procesamiento de las comunicaciones por satélite ("performing satellite communication processing"), prestar servicios de criptografía y de comunicación ("cryptologic and communications service") y apoyar las

[38] „It provides enhhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded filed stations.“ Pagina web del 544^{oh} Grupo de Inteligencia http://www.aia.af.mil

labores de la Marina y del Ministerio de Defensa (entre otros aspecto, la recogida de informaciones COMSAT) (detalles sobre el 544º GI). Sábana Seca deberá convertirse en el futuro en la primera estación de análisis y de procesamiento de las comunicaciones por satélite.

Morwenstow, Inglaterra (4ºO, 51ºN)

Morwenstow, al igual que Yakima, se fundó a principios de los años 70, coincidiendo con la primera generación de satélites INTELSAT. El operador de Morwenstow es el servicio de inteligencia británico (GCHQ). En Morwenstow existen, aproximadamente, 30 antenas de satélite, dos de las cuales tienen un diámetro de 30 m; no se dispone de datos en cuanto al tamaño de las demás antenas.

Oficialmente, no se conocen los cometidos de la estación; el tamaño, el número de las antenas de satélite y su situación sólo a 110 km. de la estación de telecomunicaciones de Goonhilly no dejan lugar a dudas acerca de su función como estación de interceptación de satélites de comunicaciones.

Menwith Hill, Inglaterra (2ºO, 53ºN)

Menwith Hill se fundó en 1956. En 1974 ya existían 8 antenas de satélite. Entretanto, el número de antenas ha aumentado a 30, aproximadamente; algunas tienen un diámetro de más de 30 m. En Menwith Hill trabajan británicos y estadounidenses juntos. Por lo que se refiere a los Estados Unidos: el NAVSECGRU, la AIA (45º IOS) el INSCOM, que está al mando de la estación. El terreno en el que se encuentra Menwith Hill pertenece al Ministerio de Defensa del Reino Unido y se alquila al Gobierno de los Estados Unidos. Según datos oficiales, el cometido de Menwith Hill consiste en "proporcionar retransmisiones rápidas por radio y realizar investigaciones sobre las comunicaciones". Según declaraciones de Richelson y la Federation of American Scientists, Menwith Hill es a la vez una estación terrestre para satélites de espionaje y una estación terrestre para satélites de comunicación rusos.

Geraldton, Australia (114ºE, 28ºS)

La estación existe desde principios de los años 90. Dirige la estación el servicio secreto australiano (DSD).Los británicos, que estaban anteriormente estacionados en Hong Kong, pertenecen ahora al personal de esta estación. Según declaraciones de Hager, existen 6 antenas de satélite, de las cuales por lo menos una tiene un diámetro de 20 m (según estimaciones); estas antenas están orientadas a satélites situados sobre el Océano Índico y a satélites situados sobre el Pacífico.

Según declaraciones realizadas por expertos bajo juramento ante el Parlamento australiano, en Geraldton se interceptan satélites de comunicaciones[30].

Pine Gap, Australia (133ºE, 23ºS)

La estación de Pine Gap se fundó en 1966. La dirige el servicio secreto australiano (DSD). Casi la mitad de las personas allí estacionadas (unas 900) son estadounidenses de la CIA y el NAVSECGRU[31].

[30] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph. gov.au/hansard.

[31] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph. gov.au/hansard.

Pine Gap tiene 18 antenas de satélite, una de las cuales tiene un diámetro de unos 30 m y otra 20 m, aproximadamente. Según datos oficiales y de distintos autores, la estación funciona desde el principio como estación terrestre para satélites SIGINT. Desde allí se controlan y se dirigen varios satélites de espionaje, cuyas señales se reciben, se procesan y se analizan. El tamaño de las antenas de satélite indica también que se interceptan satélites de comunicaciones, dado que los satélites SIGINT no requieren grandes antenas de satélite. Hasta 1980, los australianos estaban excluidos del departamento de análisis de señales. Desde entonces tienen libre acceso a todas las instalaciones, excepto al servicio de criptografía de los estadounidenses.

Misawa, Japón (141ºE, 40ºN)
La estación de Misawa existe desde 1948. En ella están estacionados japoneses y estadounidenses. Por lo que se refiere a los Estados Unidos, el NAVSECGRU, el INSCOM y algunos grupos de la AIA (544º IG, 301º IS). En su terreno se encuentran, aproximadamente 14 antenas de satélite, algunas de las cuales tienen un diámetro de unos 20 m (según estimaciones). Misawa sirve oficialmente como "Cryptology Operations Center" (Centro de operaciones de criptografía). Según declaraciones de Richelson se interceptan, con ayuda de Misawa los satélites Molnyia rusos y otros satélites rusos de comunicaciones.

Waihopai, Nueva Zelanda (173ºE, 41ºS)
Waihopai existe desde 1989. Desde entonces funciona una gran antena de 18 m de diámetro; posteriormente se añadió otra antena más pequeña. Según Hager la antena grande está orientada a INTELSAT 701 sobre el Pacífico.

Buckley Field, USA, Denver, Colorado (104ºO, 40ºN)
La estación se fundó en 1972. Allí se encuentra estacionado el 544º IG (destacamento 45). En su terreno se sitúan, aproximadamente, 5 antenas de satélite, 4 de las cuales tienen un diámetro de unos 20 m. El cometido oficial de la estación consiste en la recopilación de datos sobre acontecimientos en el ámbito nuclear obtenidos mediante satélites SIGINT, en su evaluación y su análisis. El tamaño de las antenas de satélite indica que se captan comunicaciones civiles.

Hong Kong (22ºN, 114ºE)
La estación se fundó a finales de los años 70 coincidiendo con la segunda generación de INTELSAT y se instalaron en ella grandes antenas de satélite. No se dispone de datos acerca de su tamaño exacto. En 1994 empezó el desmantelamiento de la estación de Hong Kong y las antenas se trasladaron a Australia. No está claro qué estaciones han asumido los cometidos de Hong Kong (Geraldton, Pine Gap o Misawa en Japón). Eventualmente, los cometidos se repartieron entre distintas estaciones.

5.3.2.3.2. Otras estaciones
No se puede saber claramente cuál es la función de las siguientes estaciones con los criterios mencionados:

Leitrim, Canadá (75ºO, 45ºN)
Leitrim forma parte de un programa de intercambio entre unidades militares canadienses y estadounidenses. En Leitrim están estacionadas, según declaraciones de la Marina estadounidense, unas 30 personas. En 1985 se instaló la primera de las cuatro antenas de satélite; las dos mayores tienen un diámetro de sólo 12 m, aproximadamente, (según estimaciones).

Los cometidos de la estación son, según los datos oficiales, "calificación criptográfica" y la interceptación de comunicaciones diplomáticas.

Bad Aibling, Alemania (12ºE, 47ºN)
La estación de Bad Aibling, en la que trabajan unos 750 estadounidenses, se transfirió al ejército de los EE.UU. en 1952 (entre 1972 y 1994 estuvo en manos del Ministerio de Defensa). Están estacionados en Bad Aibling el NAVSECGRU, el INSCOM (66º IG, 718 IG) y distintos grupos de la AIA (402º IG, 26º IOG). La estación posee 14 antenas de satélite de las que ninguna tiene más de 18 m; según datos oficiales los cometidos de Bad Aibling son: "Rapid Radio Relay and Secure Commo, Support to DoD and Unified Commands, Medium and Longhand Commo HF& Satellite, Communication Physics Research, Test and Evaluate Commo Equipment". Según Richelson, la estación terrestre de Bad Aibling se encarga de los satélites SIGINT y los satélites de comunicaciones rusos.

Ayios Nikolaos, Chipre (32º E, 35ºN)
Ayios Nikolaos, de Chipre, es una estación británica. Los cometidos de la estación, que tiene 9 antenas de satélite cuyo tamaño no se conoce, se reparten en dos unidades: el "Signals Regiment Radio" y la "Signals Unit (RAF)".

La situación de Agios Nikolaos, próxima a los Estados árabes, y el hecho de que es la única estación en algunas huellas de satélite (sobre todo sub-haces) en cuya zona se encuentra, indican que esta estación desempeña un papel importante en el suministro de información.

Shoal Bay, Australia (134ºE, 13ºS)
Shoal Bay es una de las estaciones gestionadas por el servicio de inteligencia australiano. La estación tiene 10 antenas de satélite, cuyo tamaño no se conoce exactamente. De las antenas de satélite que se ven en las fotografías, las mayores tienen un diámetro de 8 m, como máximo. La sexta visible es aún más pequeña. Según los datos de Richelson las antenas están orientadas hacia los satélites PALAPA indonesios. No está claro si la estación forma parte de un sistema mundial de interceptación de comunicaciones civiles.

Guam, Pacífico (144ºE, 13ºS)
Guam existe desde 1898. Hoy en día alberga una estación naval de ordenadores y telecomunicaciones, en la que están estacionados la 544º IG de la AIA y soldados de la Marina estadounidense. Existen en la estación por lo menos 2 antenas de satélite cuyo tamaño no se conoce. Así pues la función de Guam no está clara.

Kunia, Hawai (158ºO, 21ºN)
Desde 1993, esta estación funciona como Centro de operaciones de seguridad regional (RSOC) y la gestionan el NAVSECGRU y la AIA. Entre sus cometidos se cuentan la preparación de información y comunicaciones, así como el apoyo criptográfico. La función de Kunia no está clara.

Medina Annex, Texas, EE.UU. (98ºO, 29ºN)
Medina es, al igual que Kunia, un Centro de operaciones de seguridad regional fundado en 1993 y gestionado por unidades del NAVSECGRU y la AIA, con misiones en el Caribe.

Fort Gordon (81ºO, 31ºN)

Fort Gordon es también un Centro de operaciones de seguridad regional, gestionado por el INSCOM y la AIA (702º IG, 721º IB, 202º IB, 31º IS) con funciones poco claras.

Fort Mead, EE.UU. (76ºO, 39ºN)
Fort Mead es la sede de la NSA.

5.3.3. Resumen de los resultados

De los datos recogidos sobre las estaciones, los satélites y las condiciones descritas pueden extraerse las siguientes conclusiones:

1. Existen en cada huella de satélite estaciones de interceptación para, por lo menos, algunos de los haces globales con una antena de 1 diámetro mayor de 18 m, como mínimo, cada una, gestionadas por estadounidenses o británicos; esto es, donde los estadounidenses o los británicos ejercen actividades de inteligencia. Ello constituye un fuerte indicio de la existencia de un sistema mundial de interceptación .
2. El desarrollo de la comunicación INTELSAT coincidiendo con la instalación de las correspondientes estaciones de interceptación prueba el carácter mundial del sistema.
3. A partir de los puntos 1 y 2 se pueden identificar claramente determinadas estaciones como estaciones que interceptan comunicaciones internacionales por satélite.
4. Los datos de los documentos desclasificados y de los operadores (AIA, NSA, Marina estadounidense, etc.) se han de considerar una prueba de la existencia de las estaciones que allí se mencionan.
5. Algunas estaciones se encuentran simultáneamente en los haces o sub-haces de distintos satélites, de modo que se puede captar una parte importante de las comunicaciones.
6. Hay otras estaciones que no disponen de grandes antenas, pero que pueden formar parte del sistema, ya que pueden captar comunicaciones de los haces y sub-haces. Aquí hay que prescindir del tamaño de las antenas como indicio y recurrir a otros indicios.
7. Existen pruebas de que otras de las estaciones mencionadas están situadas en las cercanías inmediatas de estaciones terrestres normales de satélites de comunicaciones.

5.4. El Acuerdo UKUSA

El Acuerdo UKUSA designa un acuerdo SIGINT firmado en 1948 por el Reino Unido, los Estados Unidos, Australia, Canadá y Nueva Zelanda.

5.4.1. El desarrollo histórico del Acuerdo UKUSA[32]

El Acuerdo UKUSA es la continuación de la cooperación, muy estrecha, entre los Estados Unidos y el Reino Unido durante la segunda guerra mundial, que ya se había perfilado en la primera guerra mundial.

La iniciativa para el establecimiento de una alianza SIGINT partió de los estadounidenses[33] en

[32] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95-109.
[33] Ibidem, p. 99: "En una reunión celebrada en Londres el 31 de agosto de 1940 entre los jefes británicos de personal

una reunión celebrada en agosto de 1940 entre los estadounidenses y los británicos. En febrero de 1941 los criptoanalistas estadounidenses entregaron una máquina de cifrado (PURPLE) al Reino Unido. En la primavera de 1941 empezó la cooperación en el ámbito criptoanalítico[34]. La cooperación en el ámbito de la inteligencia se reforzó con la intervención conjunta de las flotas en el Atlántico Norte durante el verano de 1941. En junio de 1941, los británicos consiguieron descifrar el código de la flota alemana ENIGMA.

La entrada de los EE.UU. en la guerra reforzó en mayor medida la cooperación SIGINT. En 1942, los criptoanalistas estadounidenses de la "Naval SIGINT Agency" empezaron a trabajar en el Reino Unido[35]. Las comunicaciones entre las "U-Boot Tracking-Rooms"(lugares de seguimiento de submarinos) en Londres, Washington y, a partir de mayo de 1943, también Ottawa en Canadá fue tan estrecha que, según declaraciones de un antiguo colaborador, trabajaban como una organización única[36].
En la primavera de 1943 se firmó el Acuerdo BRUSA-SIGINT y se inició un intercambio de personal. El acuerdo se refiere, entre otras cosas, al reparto del trabajo y se resume en sus tres primeras frases: tiene por objeto el intercambio de toda información relativa al descubrimiento, identificación e interceptación de señales, así como el desciframiento de los códigos y claves. Los estadounidenses eran los principales responsables para el Japón y los británicos para Alemania e Italia[37].

Tras la guerra, la iniciativa de la continuación de la Alianza SIGINT partió básicamente del Reino Unido. Las bases para ello se acordaron en una gira mundial realizada en la primavera de 1945 por los miembros británicos de los servicios de inteligencia (entre otros, Sir Harry Hinsley), en cuyos libros se basa el artículo citado. Uno de los objetivos era enviar personal europeo al Pacífico para la guerra con el Japón. En este contexto, se acordó con Australia poner recursos y personal (británicos) a disposición los servicios australianos. Durante el viaje de vuelta a los EE.UU., Hinsley pasó por Nueva Zelanda y Canadá.
En septiembre de 1945, Truman firmó un memorandum altamente confidencial que constituye la pieza clave de la Alianza SIGINT en tiempos de paz[38]. A raíz de ello, se entablaron negociaciones para un acuerdo entre los británicos y los estadounidenses. Además, una delegación británica inició contactos con los canadienses y los australianos sobre una posible participación. En febrero y marzo de 1946, se celebró con el mayor secreto una conferencia

---

y la Misión de observación militar estadounidense, el representante del ejército de los EE.UU., Brigadier General George V. Strong informó de que se había acordado, en principio, entre los gobiernos EE.UU. y británico, que sería de desear un intercambio periódico de información y afirmó que había llegado el momento de proceder a un intercambio libre de inteligencia". (COS (40)289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, pp. 38, 43-4. Sir F. H. Hinsley, et al., British Intelligence in the Second World War, vol.I, pp. 312-13).

[34] Ibidem, p. 100: "En la primavera de 1941, Steward Menzies, el Jefe del SIS, designó un oficial de enlace del SIS con la British Joint Services Mission en Washington, Tim O'Connor, …, para que le asesorara en la colaboración en materia de criptología".

[35] Ibidem, p. 100 (Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol. II, p. 56.

[36] Ibidem, p. 100 (Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol. II, p. 48.

[37] Ibidem, p. 101-2: entrevistas con Sir F.H. Hinsley, "Operations of the Military Intelligence Services War Department London (MIS WD London)", 11 June 1945, Tab A, RG 457 SRH-110, NAW.

[38] Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 sept. 1945: Se autoriza al Ministro de la guerra y al Ministro de la Marina a ordenar al Director de personal del ejército de los EE.UU. y al Comandante en Jefe de la Marina de los EE.UU, así como al Director de las operaciones navales, a proseguir la colaboración en el ámbito de la inteligencia de las comunicaciones entre el ejército y la armada de los EE.UU. y los británicos y a ampliar, modificar o interrumpir esta colaboración en interés de los EE.UU." (de Bradley F. Smith, The Ultra-magic Deals and the Most Secret Spaecial Relationship (Novato, Ca:Presidio 1993).

SIGINT angloamericana para negociar los detalles. Los británicos recibieron autorización de los canadienses y los australianos. El resultado de la conferencia fue un documento, aún clasificado, de unas 25 páginas, con los pormenores de un acuerdo SIGINT entre los EE.UU y la Commonwealth británica. En los dos años siguientes se produjeron otras negociaciones que desembocarían en la firma del texto definitivo del llamado Acuerdo UKUSA en junio de 1948[39].

5.4.2. Pruebas de la existencia del acuerdo

Hasta el momento no ha habido ningún reconocimiento oficial del acuerdo UKUSA por parte de los Estados signatarios, pero existen pruebas claras de su existencia.

5.4.2.1. La lista de acrónimos de la Marina de los EE.UU.

Según la armada de los EE.UU[40], UKUSA significa "United Kingdom- USA" y designa a un "acuerdo de cinco Estados SIGINT".

5.4.2.2. Declaraciones del Director del DSD

El Director del servicio de inteligencia australiano (DSD) confirmó la existencia de este acuerdo en una entrevista. Según él, el servicio de inteligencia australiano colabora con otros servicios de inteligencia de ultramar en el marco del acuerdo UKUSA[41].

5.4.5.3. Informe de la comisión parlamentaria de inteligencia y seguridad canadiense

En este informe, se afirma que el Canadá colabora con sus aliados más firmes y antiguos en cuestiones de inteligencia. El informe los nombra: los Estados Unidos (NSA), el Reino Unido (GCHQ), Australia (DSD) y Nueva Zelanda (GCSB). El nombre del acuerdo no se menciona en el informe.

5.4.2.4. Declaraciones del antiguo Director suplente de la NSA, Louis Torella

En una entrevista con Christopher Andrew, profesor de la Universidad de Cambridge, en noviembre de 1987 y abril de 1992, el antiguo Director suplente de la NSA, Louis Torella, que estaba presente en el momento de la firma, confirma la existencia del acuerdo[42].

5.4.2.5. Carta del antiguo Director del GCHQ, Joe Hooper

El antiguo Director del GCHQ, Joe Hooper, menciona el Acuerdo UKUSA en una carta al antiguo Director de la NSA, Marshall S. Carter.

---

[39] Christopher Andrew: "The making of the Anglo-American SIGINT Alliance" en Hayden, H. Peake and S. Halpern eds. In the name of Intelligence. Essays in honor of Washington Pforzeimer (Washington NIBC Press 1995) pp. 95-109: entrevistas with Sir Harry Hinsley, March/April 1994, que participó en parte de las negociaciones; entrevistas con Louis Tordella, Director suplente de la NSA de 1958 a 1974, que estaba presente en la firma.

[40] "Terms/Abbreviations/Acronyms", publicado por la Marina de los EE.UU y el Marine Corps Intelligence Training Centre (NMITC) en http://www.cnet.navy.mil/nmitc7taining/Uniónhtml

[41] Martin Brady, Director del DSD, Canberra, 16 de marzo de 2000.

[42] Andrew, Christopher: "The growth of the Australian Intelligence Community and the Anglo-American connection", pp 223-224.

5.4.2.6. Conversaciones del ponente con otras personas

Este ponente ha mantenido conversaciones con otras personas que, por sus funciones, deben conocer el Acuerdo UKUSA y su contenido. En estas conversaciones se ha confirmado su existencia en todos los casos, indirectamente, por el tipo de respuesta.

5.5. Evaluación de documentos estadounidenses desclasificados

5.5.1. Naturaleza de los documentos

De conformidad con las "Freedom of Information Acts" (Leyes sobre la libertad de información) de 1966 (5 USC § 552) y el Reglamento del Ministerio de Defensa (Reglamento FOIA del DoD 5400.7-R, de 1997) se desclasificaron documentos que antes estaban clasificados y se permitió al público acceder a ellos.
El público puede acceder a estos documentos a través del National Security Archive de la Universidad George Washington en Washington DC. El autor Jeffrey Richelson, antiguo miembro del National Security Archive, hizo públicos, vía Internet, 16 documentos que proporcionan información general sobre el origen, el desarrollo, la gestión y los poderes de la NSA (National Security Agency)[43]. ECHELON se menciona en dos de estos documentos. Estos documentos los mencionan continuamente distintos autores que han escrito sobre ECHELON, aduciéndolos como prueba de la existencia del sistema de espionaje mundial ECHELON. Por otra parte, algunos de los documentos proporcionados por Richelson confirman la existencia de la NRO (National Reconnaissance Office) y describen su función, que consiste en administrar y explotar los satélites SIGINT[44]

5.5.2. Contenido de los documentos

Los documentos contienen descripciones fragmentarias o referencias a los siguientes temas:

5.5.2.1. Función y estructura de la NSA (documentos 1, 4, 10, 11 y 16)

En la Directiva 9 del National Security Council Intelligence (NSCID9) de 10 de marzo de 1950, se define el concepto de comunicación exterior para los fines del COMINT; así, por **comunicación exterior hay que entender toda comunicación gubernamental en sentido amplio (no sólo militar) y toda otra comunicación que pueda contener información de interés militar, político, científico o económico.**

La Directiva (NSCID 9 rev. 29.12.52) declara expresamente que sólo el FBI es responsable de la seguridad interna.

La Directiva (DoD) del Ministerio de Defensa de 23 de diciembre de 1991sobre la NSA y el Servicio Central de Seguridad (CSS) resume la estructura de la NSA de la manera siguiente:
- La NSA es una oficina organizada de manera independiente en el Ministerio de Defensa y dirigida por el Secretario de Defensa;

[43] http:www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[44] http:www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.htm

- La NSA asume en primer lugar la misión SIGINT de los EE.UU y proporciona, en segundo lugar, sistemas seguros de comunicaciones para todos los departamentos y servicios;
- Las actividades de la NSA por lo que se refiere a SIGINT no cubren la producción y distribución de la información ya tratada: esto incumbe a otros departamentos y servicios.

La Directiva del Ministerio de Defensa de 1991 esboza también la estructura la NSA el CSS.

En su declaración realizada el 12 de abril de 2000 ante el "House Permanent Select Committee on Intelligence", el Director de la NSA, Sr. Hayden, definió las tareas de la NSA del siguiente modo:
- La NSA recoge comunicaciones exteriores para los responsables militares y políticos mediante la vigilancia electrónica;
- La NSA suministra inteligencia para el Gobierno de los EE.UU. sobre el terrorismo internacional, las drogas y la proliferación de armamentística;
- La NSA no tiene el cometido de recoger todas las comunicaciones electrónicas.
- La NSA sólo puede transmitir información a destinatarios autorizados por el Gobierno y no directamente a empresas de los EE.UU..

En un memorándum redactado el 8 de abril de 1992 por el Vicealmirante W.O. Studeman, de la Marina de los EE.UU., en nombre del Gobierno, se hace referencia al carácter cada vez más internacional de la misión de la NSA (access), junto con el "apoyo a operaciones militares".

5.5.2.2. Poderes de los organismos de inteligencia (documento 7)

De la Directiva 18 de la United States Signals Intelligence (USSID) se desprende que se interceptan tanto las señales transmitidas por cable como las señales de radio.

5.5.2.3. Cooperación con otros servicios (documentos 2a y 2b)

Las tareas del Communications Intelligence Board de los EE.UU. incluyen la supervisión de todos los acuerdos con gobiernos extranjeros en el campo COMINT. Una de las tareas del director de la NSA consiste en organizar los contactos con los servicios COMINT extranjeros.

5.5.2.4. Mención de unidades activas en los emplazamientos ECHELON (documentos 9 y 12)

En las NAVSECGRU INSTRUCTIONS C5450.48A se describen los cometidos, la función y el propósito de la actividad del Naval Security Group (NAVSECGRUACT), 540º grupo de inteligencia, en Sugar Grove, West Virginia. Aquí se detalla que un cometido específico consiste en administrar y explotar un emplazamiento ECHELON; otro de los cometidos que se mencionan es el del tratamiento de la información procedente de los servicios de inteligencia.

En el documento "History of the Air Intelligence Agency-1 January to 31 December 1994" (RCS: HAF-HO (A&SA) 7101, volumen 1) se afirma, en el capítulo "Activation of Echelon Units" de la Air Intelligence Agency (AIA) , destacamentos 2 y 3 lo siguiente:

Estos documentos no proporcionan información alguna sobre lo que es un emplazamiento ECHELON, sobre lo que se hace en un emplazamiento ECHELON ni sobre qué significa la

denominación ECHELON. Los documentos no permiten saber nada acerca del acuerdo UKUSA:

5.5.2.5. Mención de estaciones (documentos 6, 9 y 12)

- Sugar Grove, West Virginia en NAVSECGRU INSTRUCTIONS C5450.48A
- Misawa , Japan in History of the Air Intelligence Agency- January to 31 December 1994 (RCS: HAF-HO (A&SA), volumen 1
- Puerto Rico (i.e, Sabana Seca), ibídem.
- Guam, ibídem.
- Yakima, Washington, ibídem.
- Fort Meade, Maryland; un informe COMINT de la NSA de Fort George G. Meade, Maryland del 31 de agosto de 1971 confirma las actividades COMINT en este lugar.

5.5.2.6. Protección de la vida privada de los ciudadanos de EE.UU. (documentos 7, 7 a a f, 11 y 16)

En las INSTRUCTIONS NAVSECGRU C5450.48A se afirma que debe protegerse la vida privada de los ciudadanos.

En distintos documentos se afirma que debe protegerse la vida privada de los ciudadanos estadounidenses y cómo debe hacerse (Baker, General Counsel, NSA, carta de 9 de septiembre de 1992, United States Signals Intelligence Directive (USSID) 18, 20 de octubre de 1980, y diversos suplementos[45].

5.5.2.7. Definiciones (documentos 4, 5a y 7)

La Directiva del ministerio de Defensa de 23 de diciembre de 1991 proporciona definiciones exactas de SIGINT, COMINT, ELINT y TELINT, al igual que la Directiva n° 6 del National Security Council Intelligence de 17 de febrero de 1972.

Según estas directivas, COMINT se refiere a la recopilación y el tratamiento de comunicaciones exteriores (realizadas por medios electromagnéticos), excluyendo la interceptación y el procesamiento de comunicaciones, prensa y propaganda escritas no cifradas.

5.5.3. Resumen

1. Hace 50 años había interés no sólo en información de las esferas política y de seguridad, sino también de la ciencia y de la economía.
2. Los documentos prueban que la NSA colabora con otros servicios en el ámbito de COMINT.
3. Los documentos que revelan información sobre cómo está organizada la NSA, así como sobre su subordinación al Ministerio de Defensa no aportan más información de la que puede extraerse

[45] Dissemination of US Government Organizatios and Officials, Memorandum 5 february 1993; Reporting Guidance on References to the First Lady, 8 July; reporting Guidance on Former President Carter's Involment in the Bosnian Peace Process, 15 December 1994; Understanding USSID 18, 30 september 1997; USSID 18 Guide 14 February 1998,

NSA/US IDENTITIES IN SIGINT, March 1994; Statement for the record of NSA Director Lt Gen. Michael V. Hayden, USAF, 12 April 2000.

de las fuentes accesibles al público en la página inicial de la NSA.
4. Las comunicaciones por cable pueden interceptarse.
5. El Intelligence Group 544 y los destacamentos 2 y 3 de la Air Intelligence Agency participan en la recopilación de información de inteligencia.
6. El término ECHELON aparece en varios contextos.
7. Para las estaciones SIGINT se mencionan: Sugar Grove en West Virgina la Misawa Air Base del Japón, Puerto Rico (Sabana Seca), Guam y Yakima en el Estado de Washington.
8. Los documentos proporcionan información sobre cómo debe protegerse la vida privada de los ciudadanos estadounidenses.

Los documentos no aportan pruebas, pero proporcionan fuertes indicios, que junto con otros, permiten extraer conclusiones.

5.6. Información procedente de autores especializados y periodistas

5.6.1. El libro de Nicky Hager

El sistema ECHELON se detalla por primera vez en el libro de Nicky Hager, "Secret Powers – New Zealand's role in the international spy network". Según Hager, sus orígenes se remontan a 1947, cuando, tras su cooperación en la guerra, el Reino Unido y los EE.UU. acordaron proseguir, conjuntamente y a escala internacional, las actividades COMINT. Ambos países debían cooperar en la creación de un sistema de interceptación tan global como fuera posible compartiendo las instalaciones especiales requeridas para ello, así como los costes, con la posibilidad de acceder conjuntamente a los resultados. Canadá, Australia y Nueva Zelanda firmaron posteriormente el acuerdo UKUSA.

Según Hager,la interceptación de comunicaciones por satélite constituye hoy en día la actividad principal del sistema.

Ya en los años 70 empezaron a interceptarse con estaciones terrestres las comunicaciones transmitidas por INTELSAT, el primer sistema mundial de telecomunicaciones por satélite[46]. A continuación, estos mensajes se estudiaban con ordenadores sobre la base de palabras clave o direcciones para filtrar los mensajes interesantes. La actividad de vigilancia se hizo extensiva después a otros satélites, como los de INMARSAT[47], que se concentraba en las comunicaciones marítimas.

En su libro, Hager señala que la interceptación de comunicaciones por satélite no representa sino una pequeña parte, aunque importante, del sistema de interceptación. Existen además numerosas instalaciones de control de los haces hertzianos y de los cables, aunque éstas no estén tan bien documentadas y su existencia sea más difícil de probar, puesto que, a diferencia de lo que ocurre con las estaciones terrestres, pueden pasar prácticamente desapercibidas. ECHELON se convierte de esta manera en sinónimo se sistema de interceptación a escala mundial.

5.6.2. Datos proporcionados por Duncan Campbell

En el estudio STOA 2/5 de 1999, que proporciona un análisis en profundidad de los aspectos

[46] Véase: www.intelsat.org/index3.htlm
[47] Véase: www.inmarsat.org/index3.htlm.

técnicos, Duncan Campbell describió detalladamente cómo se puede interceptar cualquier medio utilizado para transmitir información. En uno de sus últimos escritos, sin embargo, deja claro que incluso ECHELON tiene sus límites y que la opinión inicial de que era posible un control total de las comunicaciones ha resultado ser errónea. "Ni ECHELON ni el sistema de espionaje electrónico del que forma parte son capaces de ello. Tampoco existen equipos con suficiente capacidad para procesar y reconocer cada mensaje vocal o cada llamada telefónica"[48].

5.6.3. Datos proporcionados por Jeff Richelson

El autor Jeff Richelson, antiguo miembro de los National Security Archives ha proporcionado acceso, por Internet, a 16 documentos que estaban clasificados. En estos documentos se resumen el origen, el desarrollo, la gestión y los poderes de la NSA (National Security Agency)[49]
Además, es autor de varios libros y artículos sobre las actividades de inteligencia de los EE.UU..
En su libro "The Ties that Bind"[50], publicado en 1985, describe pomenorizadamente cómo surgió el acuerdo UKUSA, así como las actividades de los servicios secretos de los EE.UU., el Reino Unido, Canadá, Australia y Nueva Zelanda que participan en el acuerdo.
En su extenso libro "The US Intelligence Community"[51] de 1999 resume las actividades de inteligencia de los EE.UU. y describe las estructuras organizativas de los servicios y sus métodos de recopilación y análisis de la información. En el capítulo 8 detalla las capacidades SIGINT de los servicios de inteligencia pory describe algunas estaciones terrestres. En el capítulo 13 describe las relaciones de los EE.UU con los servicios de inteligencia de otros países, incluido el Acuerdo UKUSA. Menciona el nombre ECHELON como palabra de acceso a un sistema de intercambio informatizado.

En su artículo "Desperately seeking Signals"[52], publicado en 2000, describe brevemente el acuerdo UKUSA, menciona instalaciones de interceptación de satélites y describe las posibilidades y los límites de la interceptación de las comunicaciones civiles.

5.6.4. Datos proporcionados por James Bamford

Se incluirán posteriormente

5.6.5. Datos proporcionados por Bo Elkjaer y Kenan Seeberg

Estos dos periodistas declararon ante la Comisión, el 22 de enero de 2001, que ECHELON ya estaba muy avanzado en los años 80 y que Dinamarca cooperaba con los EE.UU. desde 1984.

[48] Duncan Campbell, Inside Echelon. Sobre la historia, la técnica y la función del sistema mundial de interceptación y filtrado conocido como Echelon, 1.
[49] http://www.gw.edu/~narchiv/NSAEBB/NSAEBB23/index.html.
[50] Jeffrey T. Richelson, Desmond Ball 1985: The Ties that Bind, Boston UNWIN HYMAN, Sydney Wellington London.
[51] Jeffrey T. Richelson 1999 (4ª edición): "The US Intelligence Community", Westiew Press.
[52] Jeffrey T. Richelson 2000: "Desperately seeking Signals", The Bulletin of the Atomic Scientists, March/April 2000, Vol.56, pp. 47-51.

5.7. Declaraciones de antiguos empleados de servicios de inteligencia

5.7.1. Margaret Newsham (antigua empleada de la NSA)

Entre 1974 y 1984, Margaret Newsham[53] colaboró con la Ford y Lockheed y, según sus propias declaraciones, trabajó para la NSA durante ese período. Se había formado para este trabajo en la sede de la NSA en Fort George Meade en Maryland, EE.UU. y, entre 977 y 1978 trabajó en Menwith Hill, la estación terrestre de los EE.UU. en territorio británico. Allí tuvo ocasión de comprobar que se interceptaba una conversación del senador de los EE.UU Strohm Thurmond. Ya en1978, ECHELON era capaz de interceptar las telecomunicaciones efectuadas por una persona vía satélite. Por lo que se refiere a su papel en el NSA, era responsable del diseño de sistemas y programas, de su configuración y de hacerlos operativos en grandes ordenadores. Los programas informáticos se llamaban SILKWORTH y SIRE, mientras que ECHELON era el nombre de la red.

5.7.2. Wayne Madsen (antiguo empleado de la NSA)

Wayne Madsen[54], antiguo empleado de la NSA, confirma también la existencia de ECHELON. Opina que la recopilación de datos económicos es prioritaria y se utiliza en beneficio de empresas de los EE.UU.. Teme en especial que ECHELON pueda espiar a ONG como Amnistía Internacional o Greenpeace. Añade que la NSA tuvo que admitir que disponía de más de 1000 páginas de información sobre la princesa Diana porque su campaña contra las minas demostraba una actitud contraria a la política de los EE.UU..

5.7.3. Mike Frost (antiguo empleado del servicio secreto canadiense)

Mike Frost trabajó durante más de 20 años para el CSE, servicio secreto canadiense[55]. La estación de interceptación de Ottawa era sólo una parte de una red internacional de estaciones de espionaje[56]. En una entrevista concedida a la CBS, declaró que "las conversaciones telefónicas, los correos electrónicos y los fax son supervisados cada día en todo el mundo por ECHELON, una red secreta de vigilancia del Gobierno"[57]. Ello afecta también a las comunicaciones civiles. En una entrevista que concedió a un canal de televisión australiano, dijo, a modo de ejemplo, que el CSE había introducido el nombre y el número de teléfono de una mujer en una base de datos de posibles terroristas porque había utilizado una frase ambigua en una conversación telefónica inofensiva con un amigo. Al buscar a través de comunicaciones interceptadas, el ordenador había encontrado la palabra clave y había reproducido la conversación. El analista, que no sabía muy bien qué pensar, registró sus datos personales[58].

Los servicios de inteligencia de los Estados de ECHELON se ayudan mutuamente: un servicio

[53] Véase, para las declaraciones que siguen, Bo Elkjaer, Kenan Seeberg, Echelon was my baby- interview with Margaret Newsham, Ekstra Bladet, 17.1.1999.
[54] Entrevista de la NBC "60 minutes" de 27.2.2000; http://cryptome.org/echelon-60min.htm.
[55] Communication Security Establishment, servicio dependiente del Ministerio de Defensa canadiense, que gestiona SIGIT.
[56] Entrevista de la NBC "60 minutes" de 27.2.2000; http://cryptome.org/echelon-60min.htm.
[57] Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit.
[58] Entrevista de la NBC "60 minutes" de 27.2.2000; http://cryptome.org/echelon-60min.htm.

espía por cuenta de otro, de modo que no se puede acusar de nada al servicio de inteligencia nacional. Por ejemplo, el GCHQ pidió al CSE canadiense que espiara a dos ministros británicos porque la Primera Ministra, Sra. Thatcher quería saber si estaban de su parte[59].

5.7.4. Fred Stock (antiguo empleado del servicio secreto canadiense)

Según sus propias declaraciones, Fred Stock fue expulsado del servicio secreto canadiense, CSE, en 1993 porque había criticado el nuevo énfasis del servicio en la información económica y los objetivos civiles. Las comunicaciones interceptadas contenían información sobre el comercio con otros países, incluidas las negociaciones sobre el NAFTA, la compra de cereales por China y las ventas de armas francesas. Según, el servicio recibía también habitualmente información sobre acciones de protesta de los ecologistas llevadas a cabo por barcos de Greenpeace en alta mar[60] .

5.8. Información de fuentes gubernamentales

5.8.1. Declaraciones estadounidenses

James Woolsey, antiguo director de la CIA, declaró en una conferencia de prensa[61]que concedió a petición del Departamento de Estado de EE.UU., que los EE.UU. llevaban a cabo operaciones de espionaje en la Europa continental. Sin embargo, el 95% de la "inteligencia económica" se obtiene evaluando públicamente fuentes de información accesibles, y solamente el 5% procede de secretos robados. La información económica de otros países es objeto de espionaje en relación con el cumplimiento de sanciones y las mercancías de doble uso, así como para combatir el soborno en la adjudicación de contratos. No obstante, esta información no se comunica a las empresas estadounidenses. Woolsey subrayó que, aunque el espionaje de datos económicos permitiera obtener información cuya utilización presentara un interés económico, un analista emplearía demasiado tiempo en analizar con este propósito el gran volumen de información disponible, y que no sería correcto que utilizara su tiempo para espiar a socios comerciales amigos. Señaló asimismo que, aunque fuera este el caso, sería difícil, habida cuenta de las complejas interdependencias internacionales, decidir qué empresas son empresas estadounidenses y se les debe transmitir la información.

En un artículo posterior para el diario Wall Street Europa, Woolsey reiteró que los EE.UU. efectuaban operaciones de espionaje en Europa, pero sólo para descubrir casos de soborno. Afirmó también con toda claridad que los EE.UU. utilizaban ordenadores para llevar a cabo búsquedas de datos por palabra clave.

5.8.2. Declaraciones británicas

Las respuestas británicas a diversas preguntas en la Cámara de los Comunes[62] revelan que la estación de la Royal Air Force (RAF) en Menwith Hill pertenece al Ministerio de Defensa británico, pero está a disposición del Ministerio de Defensa de los EE.UU., en particular la

[59] Entrevista de la cadena australliana Channel 9 de 23.3.1999.
[60] Bronskill, canadá a key snooper in huge spy network, Ottawa citizen, 24.10.2000, http://www.ottawacitizen.com.national/990522/2630510.html.
[61] transcript. 7.3.2000, http://cryptome.org./echelon-cia.html.
[62] Common Writen Answers, House of Commons Hansard Dedares.

NSA[63], uno de cuyos miembros dirige la estación[64], como instalación de comunicaciones[65]. A mediados de 2000, había en Menwith Hill 415 militares de los EE.UU, 5 del Reino Unido, 989 civiles de los EE.UU. y 392 civiles británicos, sin contar el personal del GCHQ[66]. La presencia de personal militar de los EE.UU. la regulan el Tratado del Atlántico Norte y los protocolos administrativos confidenciales especiales[67] , que se consideran apropiados para la relación que existe entre los Gobiernos del Reino Unido y los EE.UU. a efectos de la defensa común[68]. La estación es parte integrante de la red mundial del Ministerio de Defensa de los EE.UU., que apoya los intereses del Reino Unido, los EE.UU. y la OTAN[69].

En el informe anual de 1999/2000 se hace hincapié en el valor de la estrecha colaboración en el marco del acuerdo UKUSA, tal como se refleja en la calidad de los resultados del servicio de inteligencia. Se señala en especial que cuando el equipo del NSA dejó de funcionar durante tres días, el GCHQ sirvió a los clientes de EE.UU. además de a los clientes británicos[70].

5.8.3. Declaraciones australianas[71]

Martin Brady, director del servicio de inteligencia australiano DSD[72], confirmó en una carta al programa "Sunday" del canal 9 de Australia que el DSD colaboró con otros servicios de inteligencia como parte del acuerdo UKUSA. En la misma carta, subrayó que las instalaciones de inteligencia de toda Australia las explotaban los servicios australianos por su cuenta o conjuntamente con los servicios de los EE.UU.. En los casos en que se compartía el uso de tales instalaciones, el Gobierno australiano tenía un conocimiento completo de todas las actividades y el personal australiano participaba a todos niveles[73].

5.8.4. Declaraciones de los Países Bajos

El 19 de enero de 2001, el Ministro de Defensa de los Países Bajos presentó un informe al Parlamento de los Países Bajos sobre los aspectos técnicos y jurídicos de la interceptación mundial de los sistemas modernos de telecomunicaciones[74]. En él, y aunque no tenía información propia al respecto, el Gobierno de los Países Bajos consideraba, sobre la base de la información disponible de terceros, que la existencia de ECHELON era altamente probable, pero que había también otros sistemas con las mismas capacidades. El Gobierno de los Países Bajos llegó a la conclusión de que la interceptación mundial de sistemas de comunicaciones no se limitaba a los países implicados en el sistema ECHELON, sino que la realizaban también los gobiernos de otros países.

---

[63] 12.7.1995.
[64] 25.10.1994.
[65] 3.12.1997.
[66] 12.5.2000.
[67] 12.7.1995.
[68] 8.3.1999, 6.7.1999
[69] 3.12.1997.
[70] Intelligence and Security Committee, Annual Report 1999-2000, Parlamento 14, presentado por el Primer Ministro al Parlamento en noviembre de 2000.
[71] http://Sunday.ninimsn.com/01_cover_stories/transcript_335.asp.
http://Sunday.ninimsn.com/01_cover_stories/article_335.asp.
[72] Defence Signals directorate, servicio de inteligencia australiano que gestiona SIGINT.
[73] Carta de Martin Brady, Director del DSD desde el 16 de marzo de 1999, a Ross Coulthart, programa Sunday; véase también : http://Sunday.ninemsn.com/o1_coverstories/transcrupt_335.asp.
[74] Carta a la Tweedw Kamer "Het grootschalig afluisteren van moderne telecommunicatiesystemen".

5.8.5. Declaraciones italianas

En la entrevista que concedió a "Il Mondo", Luigi Ramponi, anterior director de SISMI, el servicio de inteligencia italiano, confirmó de manera tajante la existencia de ECHELON[75] Ramponi afirmó explícitamente que, como jefe de SISMI, supo de la existencia de ECHELON. Desde 1992, estaba al corriente de la existencia de una importante actividad de interceptación de ondas de baja, media y alta frecuencia. Cuando empezó en el SISMI en 1991, casi todo el trabajo que se hacía estaba relacionado con el Reino Unido y los EE.UU..

5.9. Informes parlamentarios

5.9.1. Informes del Comité Permanente R (comisión de control belga)

La comisión de control belga (Comité Permanente R) se ha manifestado ya mediante dos informes sobre el asunto ECHELON.

En el informe "Rapport d'activités 1999" se dedica el capítulo 3 a la cuestión de cómo reaccionan los servicios secretos de información belgas ante la posible existencia de un sistema de vigilancia de las comunicaciones ECHELON. En el informe, de 15 páginas, se llega a la conclusión de que los dos servicios secretos de información belgas, Sûreté de l'Etat y Service Général du Renseignemnet (SGR), sólo obtuvieron información relativa a ECHELON a través de documentos públicos.

El segundo informe "Rapport complémentaire d'activités 1999" se ocupa fundamentalmente de forma pormenorizada del sistema ECHELON. En él se emite una opinión sobre el estudio STOA y se dedica una parte de la explicación a la descripción de las condiciones generales técnicas y jurídicas de la interceptación de las telecomunicaciones. Sus conclusiones indican que ECHELON existe realmente y tiene capacidad para interceptar toda la información transmitida vía satélite (aproximadamente un 1% de todas las llamadas internacionales), siempre que se realice una búsqueda mediante palabras clave, y que sus capacidades en lo relativo a la descodificación son muy superiores a lo indicado por parte de los Estados Unidos. Existen dudas con respecto a las declaraciones de que en Menwith Hill no se ejerce espionaje industrial. Se subraya expresamente que no se puede determinar con seguridad lo que hace o no hace ECHELON.

5.9.2. Informe de la Comisión de defensa nacional de la Asamblea Nacional francesa

En Francia, la Comisión de Defensa Nacional presentó a la Asamblea Nacional un informe relativo a los sistemas de interceptación.[76]

---

[75] Francesco Sorti, Dossier.exclusivo.caso Echelon. Parla Luigi Ramponi. Anche i politici sapevano, Il mondo, 17.4.1998

[76] Documento informativo presentado en cumplimiento del artículo 145 del Reglamento por la Comisión de Defensa Nacional y de las Fuerzas Armadas sobre los sistemas de vigilancia e interceptación electrónica que puedan poner en peligro la seguridad nacional, n° 2623, Asamblea Nacional, registrado en la Presidencia de la Asamblea Nacional el 11 de octubre de 2000.

Tras una detallado debate sobre los diferentes aspectos, el ponente Arthur Paecht llega a la conclusión de que ECHELON existe y de que se trata del único sistema de vigilancia multinacional conocido por él. La capacidad del sistema es real, aunque ha alcanzado sus límites, no sólo debido a que el gasto efectivo ya no está a la altura de la explosión que se ha producido en el aumento de las telecomunicaciones, sino, además, porque determinados objetivos han aprendido a protegerse.

El sistema ECHELON ha abandonado sus objetivos originales, vinculados al contexto de la guerra fría, de forma que cabe la posibilidad de que la información recopilada con fines políticos y económicos sea utilizada en contra de otros Estados de la OTAN.

ECHELON podría constituir de forma clara un riesgo para las libertades fundamentales, surgiendo a este respecto numerosos problemas que requerirían respuestas específicas. Es un error pensar que los Estados que forman parte de ECHELON vayan a renunciar a sus actividades y los indicios parecen señalar más bien la creación de un nuevo sistema con nuevos socios y con nuevos recursos para superar los límites de ECHELON.

6. ¿Puede haber otros sistemas mundiales de interceptación?

6.1. Condiciones para este sistema

6.1.1. Condiciones técnicas y geográficas

La interceptación de comunicaciones internacionales transmitidas por satélites de primera generación requiere estaciones de recepción en el Atlántico, el Océano Índico y la zona del Pacífico. En el caso de la última generación de satélites, que pueden transmitir a subzonas, hay que cumplir otros requisitos por lo que se refiere a la posición geográfica de las estaciones de interceptación, si se pretende interceptar todas las comunicaciones vía satélite.

Otro sistema de interceptación a escala mundial debería instalar sus estaciones fuera del territorio de los Estados de ECHELON.

6.1.2. Condiciones políticas y económicas

El establecimiento de un sistema de interceptación de esta clase que funcionara a escala mundial, debería tener también sentido económico y político para el operador o los operadores. El beneficiario o los beneficiarios del sistema deben tener intereses económicos, militares u otros intereses globales en términos de seguridad, o creer por lo menos que forman parte de las superpotencias mundiales. Por lo tanto, el conjunto de países interesados se limita la China y los Estados del G-8, , sin contar a los EE.UU. y al Reino Unido.

6.2. Francia

Francia tiene sus propios territorios, departamentos y corporaciones regionales en las tres zonas enumeradas.

En el Atlántico se encuentran, al este del Canadá, Saint Pierre et Miquelon (65º O/47º N), al noreste de Sudamérica, Guadalupe (61º O/16º N) y Martinica (60º O/14º N) y, en la costa noreste de Sudamérica, la Guyana francesa (52º O/5º N).

En el Océano Índico se encuentran, al este del África meridional, Mayotte (45º E/12º S) y La Reunión (55º E/20º S), y al sur los territorios australes y antárticos franceses. En el Pacífico están Nueva Caledonia (165º E/20º S), Wallis y Futuna (176º O/12º S), así como la Polinesia francesa (150º O/16º S).

Se dispone de muy poca información sobre la posible existencia de estaciones gestionadas por el servicio de inteligencia francés (Direction générale de la securité exterieure) (DGSE) en estas zonas de ultramar. Según los informes de periodistas franceses[77], hay estaciones en Kourou en la Guyana francesa y en Mayotte. No se dispone de datos en cuanto al tamaño de las estaciones, al número de antenas por satélite o a su tamaño. Al parecer, hay otras estaciones en Francia: en Domme, cerca de Burdeos, y en Alluetts-le-Roi, cerca de París. Jauvert calcula que hay un total de 30 platos de satélite. El autor Schmidt-Enboom[78] afirma que también funciona una estación en Nueva Caledonia.

En teoría, Francia podría gestionar también un sistema mundial de interceptación. Sin embargo, este ponente no dispone de suficiente información oficialmente accesible para poder afirmarlo de manera concluyente.

6.3. Rusia

El servicio de inteligencia ruso FAPSI, que es responsable de la seguridad de las comunicaciones y de SIGINT, gestiona al parecer estaciones terrestres en Letonia, Vietnam y Cuba, en cooperación con el servicio de inteligencia militar ruso GRU.

Según la Federation of American Scientists, en la zona atlántica hay una instalación en Lourdes, Cuba (82º O/23º N), que se gestiona conjuntamente con el servicio de inteligencia cubano. En la zona del Océano Índico hay estaciones en Rusia, sobre las que no se tiene más información, y

[77] Jean Guisnel, L'éspionage n'est plus un secret, The Tocqueville Connection, 10.7.1998.
Vincent Jauvert, Espionnage comment la france, Le Nouvel Observateur, 5.4.2001, nº 1999, p. 14 y siguientes.
[78] E. Schmidt-Eenboom, en: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg 1999, p. 180.

una estación en Skundra, Letonia. En el Pacífico hay, al parecer, una estación en Cam Rank Bay, en Vietnam del Norte. No se conocen detalles por lo que se refiere al número y al tamaño de las antenas.

Junto con las estaciones disponibles en la misma Rusia, la cobertura mundial es teóricamente posible. Sin embargo, tampoco aquí la información disponible es insuficiente para extraer conclusiones fiables.

6.4. Los demás Estados del G-8 y China

Ni los demás Estados del G-8 ni China tienen territorio propio o aliados firmes en las partes del mundo necesarias para gestionar un sistema mundial de interceptación.

7. La compatibilidad de un sistema de interceptación de comunicaciones del tipo "ECHELON" con el Derecho de la Unión

7.1. Comentarios sobre la cuestión

El mandato de la comisión comprende, entre otras cosas, la tarea expresa de examinar la compatibilidad de un sistema de interceptación de comunicaciones del tipo "ECHELON" con el Derecho comunitario[79]. Deberá evaluarse, en particular, si tal sistema es compatible con las dos directivas sobre la protección de datos 95/46/CE y 97/66/CE, con el artículo 286 del TCE y con el apartado 2 del artículo 8 del TUE.

Parece necesario efectuar el examen de acuerdo con dos perspectivas diferentes. El primer aspecto se desprende del indicio indicado en el Capítulo 5, del que se desprende que el sistema denominado "ECHELON" se concibió como un sistema de interceptación de comunicaciones destinado a facilitar información a los servicios secretos norteamericanos, canadienses, australianos, neocelandeses y británicos mediante la recogida y evaluación de datos de comunicación. Se trata, por consiguiente, de un instrumento clásico de espionaje de los servicios de inteligencia extranjeros[80]. En una primera fase, deberá examinarse la compatibilidad de un sistema de servicio de inteligencia de tal tipo con el Derecho de la Unión.

Además, en el informe presentado por Campbell en el marco de STOA, se reprocha que este sistema se emplee indebidamente para espionaje en materia de competencia y que la economía de los países europeos, en consecuencia, haya sufrido grandes pérdidas. Además, de acuerdo con las declaraciones del anterior director de la CIA, R. James Woolsey, los EE. UU., ciertamente, espían a las empresas europeas, pero únicamente para restablecer la justicia en el mercado, ya que los contratos únicamente se consiguen mediante soborno[81]. En caso de que fuera cierto que se utilizan sistemas para el espionaje en materia de competencia, la cuestión de su compatibilidad con el Derecho comunitario adquiere nuevas dimensiones. Por consiguiente, este segundo aspecto deberá examinarse por separado en una fase ulterior.

7.2. La compatibilidad de un sistema de inteligencia con el Derecho de la Unión

7.2.1. Compatibilidad con el Derecho de la CE

Las actividades y acciones al servicio de la seguridad estatal, por ejemplo, la persecución del delito, no inciden directamente en el ámbito normativo del Tratado de la CE. Puesto que la Comunidad Europea, en virtud del principio de competencias limitadas, únicamente puede actuar allí donde tiene una competencia al respecto, ha excluido consecuentemente estos ámbitos de aplicación de las directivas sobre la protección de datos basadas en el Tratado CE, en particular su artículo 95 (antiguo artículo 100). La Directiva 95/46/CE relativa a la protección de las

[79] Cf. capítulo 1, 1.3.
[80] Cf. capítulo 2.
[81] Cf. capítulo 5, 5.6 y 5.8.

personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[82] y la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[83] no se aplican "en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento[84]/actividades[85] estén relacionados con la seguridad del Estado) y las actividades del Estado en materia penal". La misma formulación se aprobó en la propuesta de directiva que examina actualmente el Parlamento relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[86]. La participación de un Estado miembro en un sistema de escucha al servicio de la seguridad estatal, por consiguiente, no puede estar en contradicción con las directivas relativas a la protección de datos.

Tampoco puede producirse una violación del artículo 286 del TCE, que amplía el ámbito de aplicación de las directivas relativas a la protección de datos a su tratamiento mediante órganos y agencias de la Comunidad. Esto mismo es aplicable al Reglamento (CE) nº 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[87]. Este Reglamento únicamente es aplicable cuando los órganos actúen en el marco del Tratado de la CE[88]. A fin de evitar malentendidos, en este punto conviene subrayar que nadie jamás ha afirmado que organismos o instituciones comunitarias hayan participado en un sistema de escucha y que el ponente tampoco posee ningún tipo de indicios a tal respecto.

7.2.2. Compatibilidad con el restante Derecho de la UE

En el ámbito del Título V (política exterior y de seguridad común) y VI (cooperación policial y judicial en materia penal) no se cuenta con disposiciones relativas a la protección de datos comparables a las directivas de la CE. El Parlamento Europeo ya ha reiterado en diferentes ocasiones[89] y la necesidad de subsanar tal laguna.

La protección de los derechos y libertades fundamentales de los ciudadanos en estos ámbitos la garantizan únicamente los artículos 6 y 7, en particular el apartado 2 del artículo 6 del TUE, en el que la Unión se compromete a respetar los derechos fundamentales, según se establecen en el Convenio Europeo para la Protección de los Derechos Humanos y en las diferentes Constituciones de los Estados miembros. Sin perjuicio del carácter vinculante de los derechos fundamentales y, en particular, del Convenio Europeo para la Protección de los Derechos Humanos para los Estados miembros (véase al respecto el capítulo 8), los derechos

[82] DO L 281 de 23.11.1991, pp. 31-50.
[83] DO L 24 de 30.1.1998, pp. 1-8.
[84] Apartado 2 del artículo 3 de la Directiva 95/46/CE.
[85] Apartado 3 del artículo 1 de la Directiva 97/66/CE.
[86] COM(2000) 385 final, DO C 365 E/223.
[87] Reglamento (CE) nº 45/2001, DO L 8 de 12.1.2001, p. 1-22.
[88] Apartado 1 del artículo 3; Compárese también el considerando 15 "Cuando las instituciones y los organismos comunitarios efectúen dicho tratamiento para el ejercicio de actividades que no pertenezcan al ámbito de aplicación del presente Reglamento, y en especial de las previstas en los Títulos V y VI del Tratado de la Unión Europea, la protección de los derechos y las libertades fundamentales de las personas se garantizará respetando el artículo 6 del Tratado de la Unión Europea."
[89] Véase, por ejemplo, el apartado 25 de la Resolución sobre el plan de acción del Consejo y de la Comisión sobre la mejor manera de aplicar las disposiciones del Tratado de Amsterdam relativas a la creación de un espacio de libertad, seguridad y justicia (13844/98 - C4-0692/98 - 98/0923(CNS)), DO C 219 de 30.7.1999, pp. 61 y siguientes.

fundamentales también son vinculantes para la Unión en su actividad legislativa y administrativa. Sin embargo, ya que a escala de la UE no existe ninguna normativa sobre la admisibilidad de la vigilancia de las telecomunicaciones con fines de seguridad o inteligencia[90], no se plantea, en principio, una violación del apartado 2 del artículo 6 del TUE.

7.3. La cuestión de la compatibilidad en caso de abuso del sistema de espionaje económico

En caso de que un Estado miembro recurriera a un sistema de interceptación que, entre otras cosas, incluyera el espionaje en materia de competencia, dotando a sus propios servicios de inteligencia de los instrumentos necesarios o poniendo a disposición su territorio a tal fin a servicios de inteligencia extranjeros, sí se produciría una violación del Derecho comunitario. De hecho, los Estados miembros, de conformidad con el artículo 10 del TCE, están comprometidos a guardarse una lealtad total, en particular, a no practicar ninguna medida que pudiera poner en peligro los objetivos del Tratado. Incluso en caso de que la interceptación de telecomunicaciones no se realice en beneficio de la economía local, (lo que, además, tendría el efecto de una ayuda estatal y vulneraría, por consiguiente, el artículo 87 del TCE), sino en favor de terceros países, tal actividad estaría en contradicción total con el principio fundamental del Tratado de la CE de un mercado común, ya que supondría una violación de la competencia.

Tal comportamiento, en opinión del ponente, supondría además una violación de la directiva sobre la protección de datos en el ámbito de las telecomunicaciones[91], ya que la cuestión de la aplicación de las directivas debe resolverse con arreglo a puntos de vista operativos y no organizatorios. Así se desprende no sólo del texto de la normativa del ámbito de aplicación, sino también del espíritu de la ley. Si los servicios de inteligencia emplean su capacidad para practicar espionaje económico, su actividad no está al servicio de la seguridad o de la persecución de delitos, sino que su objetivo se ha desvirtuado e incide, por consiguiente, plenamente en el ámbito de aplicación de la Directiva. Ésta obliga a los Estados miembros en su artículo 5 a asegurar la confidencialidad de las comunicaciones, en particular, "la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios". De conformidad con el artículo 14, únicamente se permitirán excepciones cuando así sea necesario por razones de seguridad del Estado, defensa y persecución policial. Puesto que el espionaje económico no está legitimado por estas excepciones, se produciría en tal caso una violación del Derecho comunitario.

---

[90] En el ámbito de la vigilancia de las telecomunicaciones, en la actualidad en el ámbito de la UE únicamente hay dos actos jurídicos, no reglamentando ninguno de ellos la cuestión de su admisibilidad:

- Resolución del Consejo de 17 de enero de 1995 sobre la interceptación legal de las telecomunicaciones (DO C 329 de 4.11.1996, pp. 1-6), conteniendo sus anexos los criterios técnicos para la realización de medidas legales de interceptación en los sistemas modernos de telecomunicaciones y
- El Acto del Consejo de 29 de mayo de 2000, por el que se celebra, de conformidad con el artículo 34 del Tratado de la Unión Europea, el convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea (DO C 197/2000, p. 1, artículo 17, letra f), en el que se establece bajo qué condiciones podrá facilitarse asistencia jurídica en materia penal con respecto a la interceptación de las telecomunicaciones. No se vulnerarán de ninguna manera los derechos de los interceptados, ya que el Estado miembro en que se encuentre el interceptado, siempre podrá negar la asistencia jurídica cuando ésta no sea conforme con el Derecho nacional.

[91] Directiva 97/66/CE, DO L 24/1988, p. 1.

7.4. Resultados

Puede afirmarse, en resumen, que, con arreglo a la actual situación jurídica, un sistema de inteligencia del tipo ECHELON no viola el Derecho de la Unión porque no posee puntos de contacto con éste, lo que sería necesario para su incompatibilidad. Pero esto es únicamente así en la medida en que el sistema realmente se emplee únicamente al servicio de la seguridad del Estado. En caso de que se le diera una utilidad distinta y se empleara para el espionaje en materia de competencia contra empresas extranjeras, esto violaría el Derecho de la CE. En caso de que participara en tal actividad un Estado miembro, éste violaría el Derecho comunitario.

8. La compatibilidad de la interceptación de las comunicaciones con los servicios de inteligencia con el derecho fundamental a la intimidad

8.1. Interceptación de las comunicaciones como injerencia en el derecho fundamental a la intimidad

Toda escucha de comunicaciones, así como la interceptación de datos mediante servicios de inteligencia con este objetivo[92] es una violación grave de la intimidad de la persona. Únicamente en un "Estado policial" es admisible la escucha ilimitada por parte del Estado. En los Estados miembros de la UE, que son democracias consolidadas, es indiscutible que los órganos estatales deben respetar la vida privada y, por consiguiente, también los servicios de inteligencia, lo que, con frecuencia, así se recoge en las constituciones de los Estados miembros. La esfera privada, por consiguiente, disfruta de una protección especial, las intervenciones se producen únicamente tras ponderar las ventajas e inconvenientes jurídicos y respetando el principio de proporcionalidad.

También en los Estados ECHELON hay conciencia del problema. Las normas protectoras previstas tienen como objetivo aquí, sin embargo, el respeto de la esfera privada de la propia población, de tal manera que los ciudadanos europeos, por lo general, no se benefician de ella. En las disposiciones de los EE. UU., por ejemplo, se reglamentan las condiciones de la vigilancia electrónica, el interés estatal en un servicio de inteligencia operativo no está en contradicción con los intereses de una protección eficaz de los derechos fundamentales elementales, sino al servicio de la protección necesaria de la esfera privada de los ciudadanos norteamericanos[93].

8.2. La protección de la esfera privada por los convenios internacionales

El respeto de la esfera privada es un derecho fundamental recogido en numerosos convenios internacionales[94]. A nivel mundial debe mencionarse, en particular, el "Pacto internacional sobre

[92] Tribunal Constitucional Federal Alemán (BVerfG), 1BvR 2226/94 de 14.7.1999, apartado 187 "injerencia ya es [...] la propia interceptación, en la medida en que la comunicación se facilite al servicio federal de inteligencia y constituya la base del modelo de conceptos de búsqueda."

[93] Cf. al respecto el informe presentado ante el Congreso norteamericano a finales de febrero de 2000 "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, impreso en el Foreign Intelligence Surveillance Act (FISA), título 50, capítulo 36 U.S. C. §1801 ss. y la Exec. Order nº 12333, 3 C.F.R. 200 (1982), capítulo 15 U.S. C. apartado 41 y siguientes, http://www4.law.cornell.edu/uscode/50/index.html.

[94] Artículo 12 de la Declaración General de Derechos Humanos; artículo 17 del Pacto Internacional de las Naciones Unidas sobre los derechos políticos y ciudadanos; artículo 7 de la Carta de la UE, artículo 8 del Convenio Europeo de Derechos Humanos; recomendación del Consejo de la OCDE sobre las directrices para la seguridad de los sistemas de información, aprobado el 26/27.11.1993 (C (92) 188/final); artículo 7 del Convenio Europeo sobre la protección de las personas en lo relativo al tratamiento automático de datos personales; cf. a este respecto el estudio encargado por STOA "Desarrollo de la tecnología de vigilancia y riesgo de abusos en la información económica; volúmenes 4/5: la legalidad de la interceptación de las comunicaciones electrónicas: una investigación sucinta de las principales cuestiones e instrumentos jurídicos con arreglo al Derecho nacional, internacional y europeo" (Chris Elliot), octubre de 1999, p. 2.

los derechos ciudadanos y políticos"[95], que se aprobó en el marco de las Naciones Unidas y garantiza en su artículo 17 la protección de la esfera privada. Todos los Estados ECHELON han respetado las decisiones de la Comisión de Derechos Humanos convencional fundada de conformidad con el artículo 41, que decide sobre las cuestiones relativas a las violaciones internacionales del Pacto, en la medida en que se trata de denuncias de otros Estados. El Protocolo adicional[96], que amplía la competencia de la Comisión de Derechos Humanos a los recursos individuales, no fue firmado por los EE. UU., de tal manera que los particulares no tienen la posibilidad de recurrir a la Comisión de Derechos Humanos en caso de que los EE.UU. violen el pacto.

A escala de la UE también se intentó lograr una protección especial de los derechos fundamentales mediante la elaboración de una "Carta de derechos fundamentales de la UE". El artículo 7 de la Carta, que lleva el título "Respeto de la vida privada y familiar", reglamenta incluso expresamente el derecho al respeto de las comunicaciones[97]. Además, en el artículo 8, se reglamenta el derecho fundamental a la "Protección de datos de carácter personal", lo que habría protegido al ciudadano particular en los casos en que sus datos se traten, de manera automatizada o no, lo que es práctica habitual en las escuchas e, incluso, lo que ocurre en el caso de las demás interceptaciones.

Hasta ahora la Carta no se ha incluido en el Tratado. Únicamente resulta vinculante para las tres instituciones, que se han comprometido a respetarla en una "declaración solemne" en el marco del Consejo Europeo de Niza: Consejo, Comisión y Parlamento. Estas tres instituciones, que sepa el ponente, no intervienen en ningún tipo de actividades de servicios secretos. Aun cuando la Carta adquirirá un pleno carácter vinculante tras su inclusión en el Tratado, también debe tenerse en cuenta su ámbito limitado de aplicación. De conformidad con el artículo 51, la Carta es vinculante "para las instituciones y órganos de la Unión ..., así como para los Estados miembros únicamente cuando apliquen el Derecho de la Unión." La Carta, por consiguiente, únicamente sería pertinente en lo relativo a las ayudas estatales y legales que vulneran la competencia (véase el capítulo 7, 7.3).

El único instrumento eficaz a escala internacional para una protección eficaz de la esfera privada es el Convenio Europeo para la protección de los Derechos Humanos.

8.3. La normativa del Convenio Europeo para la Protección de los Derechos Humanos (CPDH)

8.3.1. La importancia del Convenio Europeo para la Protección de los Derechos Humanos en la UE

La protección de los derechos fundamentales prevista en el Convenio europeo tiene una importancia particular, ya que ha sido ratificado por todos los Estados miembros de la UE y, por consiguiente, ofrece un nivel unitario europeo de protección. Los Estados contractuales se han comprometido internacionalmente a garantizar los derechos previstos en el Convenio Europeo

[95] Pacto Internacional sobre los derechos políticos y ciudadanos, aprobado por la Asamblea General de las Naciones Unidas el 9 de diciembre de 1966.
[96] Protocolo facultativo al Pacto internacional sobre los derechos políticos y ciudadanos, aprobado por la Asamblea General de las Naciones Unidas el 19.12.1966.
[97] "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones."

para la protección de los derechos humanos y se han sometido a la jurisprudencia del Tribunal de Justicia Europeo de Derechos Humanos de Estrasburgo. Las diferentes normas nacionales, por consiguiente, pueden ser examinadas por el Tribunal de Estrasburgo a fin de comprobar su conformidad con el Convenio europeo y condenar a los Estados contractuales por violaciones de los derechos humanos y obligarles a pagar compensaciones. Además, el Convenio Europeo para la Protección de los Derechos Humanos adquirió más importancia, ya que en repetidas ocasiones el TJCE en el marco del examen de la legislación lo ha tenido en cuenta conjuntamente con los principios jurídicos generales de los Estados miembros a la hora de dictar sus sentencias. Además, en el Tratado de Amsterdam, en el apartado 2 del artículo 6 del TUE se incluyen las obligaciones de la UE de respetar los derechos humanos previstos en el Convenio Europeo para la Protección de los Derechos Humanos.

8.3.2. El ámbito de protección espacial y personal del CPDH

Los derechos establecidos en el CPDH son derechos fundamentales generales y, por consiguiente, no están vinculados a una nacionalidad. Deben garantizarse a todas las personas sometidas a la jurisdicción de los Estados contractuales. Esto significa que los derechos humanos deben respetarse en todo el territorio estatal y que las excepciones locales constituyen una violación contractual. Además, también tienen vigor fuera del territorio de los Estados parte, en la medida en que allí se ejerza el poder del Estado. Los derechos garantizados por el CPDH en un Estado contractual también pueden disfrutarlos las personas fuera del territorio del Estado, cuando un Estado contractual viole su esfera privada fuera de su territorio[98].

Esto último resulta particularmente importante, porque la problemática de los derechos humanos en el ámbito de la interceptación de las telecomunicaciones tiene la peculiaridad de que el Estado responsable de la vigilancia, el vigilado y el acto real de interceptación pueden producirse en diferentes lugares. Esto es particularmente cierto en el caso de las comunicaciones internacionales, pero, en determinadas circunstancias, también en las comunicaciones nacionales, cuando la información se realiza por canales en el extranjero. En el caso de los servicios extranjeros de inteligencia, éste es, incluso, el caso típico. Tampoco puede excluirse que la información resultante de las escuchas que ha obtenido un servicio de inteligencia no se facilite a otro Estado.

8.3.3. La admisibilidad de la interceptación de las telecomunicaciones de conformidad con el artículo 8 del CPDH

De conformidad con el apartado 1 del artículo 8 del CPDH “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y su correspondencia.” La protección de la telefonía o de las telecomunicaciones no se menciona expresamente, pero de conformidad con la jurisprudencia del Tribunal de Estrasburgo también están incluidas en el concepto de “vida privada” y “correspondencia” previstas en el artículo 8 del CPDH[99]. El ámbito de protección del derecho fundamental no comprende únicamente el contenido de las comunicaciones, sino

[98] Cf. al respecto TEDH, Loizidou/Türkei, 23.3.1995, apartado 62 con más pruebas "...the concept of 'jurisdiction' under this provision is not restricted to the national territory of the High Contracting Parties.[...] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory" con referencia al TEDH, Drozd y Janousek, 26.6.1992, apartado 91. Cf. al respecto exhaustivamente Jacobs, el Convenio Europeo de Derechos Humanos (1996), pp. 21 y ss.
[99] Cf. al respecto TEDH, Klass y otros, 6.9.1978, apartado 41.

también la grabación de datos ajenos a la conversación. Esto significa que incluso cuando los servicios de inteligencia únicamente registren datos como la hora y la duración de las comunicaciones, así como los números llamados, esto es una injerencia en la vida privada[100].

De conformidad con el apartado 2 del artículo 8, el derecho fundamental del CPDH no se concede sin limitaciones. Son admisibles las injerencias en el derecho fundamental al respeto de la vida privada cuando éstas tenga un fundamento jurídico en el Derecho nacional[101]. El derecho debe ser de acceso general y sus consecuencias deben ser previsibles[102].

Los Estados miembros no son libres a la hora de realizar tales injerencias. El artículo 8 del CPDH únicamente permite tales injerencias para conseguir los objetivos enumerados en el apartado 2, que son, en particular, la seguridad nacional, el orden público, la prevención de actos delictivos, así como el bienestar económico del país[103], lo que ciertamente no justifica el espionaje industrial, ya que únicamente comprende las injerencias "necesarias en una sociedad democrática". En toda injerencia debe usarse el instrumento menos lesivo para la consecución de los objetivos, debiendo existir además garantías suficientes contra los abusos.

8.3.4. La importancia del artículo 8 del CPDH para la actividad de los servicios de inteligencia

Estos principios fundamentales significan para la estructura de la actividad de los servicios de inteligencia conforme con los derechos fundamentales lo siguiente: si para garantizar la seguridad nacional resulta necesario que los servicios de inteligencia intercepten el contenido de las telecomunicaciones o, por lo menos, los datos de las conexiones, así debe reflejarse en el Derecho nacional y dicha regla debe ser de acceso público. Las consecuencias de tal actividad deberán ser previsibles para el particular, si bien deberán tenerse en cuenta los requisitos particulares de la confidencialidad. Por consiguiente, el Tribunal de Justicia en una sentencia sobre la conformidad de los controles secretos empleados en ámbitos que afectan a la seguridad nacional ha comprobado que el derecho a la previsibilidad en este caso especial no puede ser el mismo que en otros ámbitos[104]. Pero también ha exigido en este caso que el Derecho debe informar bajo qué condiciones o circunstancias el poder estatal puede realizar una injerencia peligrosa en la esfera privada[105].

En el caso de la estructura conforme a los derechos humanos de la actividad de los servicios de inteligencia debe tenerse en cuenta que la seguridad nacional es un motivo de justificación, pero

---

[100] Cf. al respecto TEDH, Malone, 2.8.1984, apartado 83 y siguientes; así como Davy, B/Davy/U, Aspectos de recopilación e información estatal y el artículo 8 del CPDH, JBI 1985, 656.

[101] De conformidad con la jurisprudencia del TEDH (en particular Sunday Times, 26.4.1979, apartado 46 y siguientes, Silver y otros, 25.3.1983, apartado 85 y siguientes), el concepto de "Derecho" del apartado 2 del artículo 8 comprende no sólo las leyes en su sentido formal sino también las disposiciones jurídicas con arreglo a su categoría en determinadas condiciones incluso el derecho consuetudinario. La condición al respecto es, sin embargo, que los sujetos pasivos del derecho sepan bajo qué condiciones es posible tal injerencia. Cf. al respecto Wessley, el secreto de las comunicaciones - ¿un derecho desconocido? ÖJZ 1999, pp. 491 y ss., 495.

[102] Silver y otros, 25.3.1983, apartado 87 y siguientes.

[103] La justificación de "bienestar económico" fue aceptada por el TEDH en un caso en el que se trataba de la transmisión de datos médicos importantes para la asignación de pagos compensatorios públicos, M. S./Schweden, 27.8.1997, apartado 38, así como en un caso en que se trataba de expulsar a una persona de los Países Bajos, que vivía de la caridad pública, tras haber perdido el derecho de residencia. Ciliz/Niederlande, 11.7.2000, apartado 65.

[104] TEDH, Leander, 26.3.1987, apartado 51.

[105] TEDH, Malone, 2.8.1984, apartado 67.

que éste de conformidad con el apartado 2 del artículo 8 del CPDH debe someterse al principio de proporcionalidad: la seguridad nacional únicamente puede justificar injerencias allí donde sean necesarias en una sociedad democrática. El Tribunal de Estrasburgo ha explicado claramente que el interés del Estado en proteger la seguridad nacional debe contraponerse a la gravedad de la injerencia en el respeto de la esfera privada del particular[106]. Ciertamente las injerencias no se reducen al mínimo imprescindible, pero los meros conceptos de utilidad o idoneidad no son suficientes[107]. La opinión de que la escucha de toda comunicación es la mejor protección contra la delincuencia organizada violaría el artículo 8 del CPDH, incluso aun cuando así lo permitiera el Derecho nacional.

Además, debido al carácter particular de la actividad de los servicios de inteligencia, que exigen confidencialidad y, por consiguiente, una particular ponderación de intereses, deben preverse mayores posibilidades de control. El Tribunal de Justicia ha indicado expresamente que un sistema secreto de vigilancia para garantizar la seguridad nacional conlleva el riesgo de que con la excusa de defender la democracia, ésta se vea socavada o incluso destruida y que, por consiguiente, se necesitan garantías más adecuadas y eficaces contra tales abusos[108]. La legítima actividad jurídica de los servicios de inteligencia, por consiguiente, únicamente se ajusta a los derechos fundamentales, cuando el Estado contractual del CPDH ha previsto suficientes sistemas de control y otras garantías contra los abusos. El Tribunal de Justicia destacó, en particular, en el contexto de la actividad de los servicios de inteligencia de Suecia, que concede particular importancia a la presencia de diputados en el órgano de control policial así como a la supervisión del ministro de Justicia, el Defensor del Pueblo parlamentario y la Comisión de Asuntos Jurídicos parlamentaria. Desde esta perspectiva, es cuestionable que Francia, Grecia, Irlanda, Luxemburgo y España no tengan una comisión parlamentaria de control propia para los servicios secretos[109] y que no conozcan un sistema de control comparable al Defensor del Pueblo parlamentario de los Estados nórdicos[110]. El ponente celebra, por consiguiente, la voluntad de la Comisión de Defensa de la Asamblea Nacional francesa de fundar una comisión de control[111], en particular porque Francia dispone de destacables capacidades de servicios de inteligencia tanto desde una perspectiva técnica como geográfica.

8.4. La obligación de prestar atención a la actividad de los servicios de inteligencia extranjeros

8.4.1. Ilegalidad de la elusión del artículo 8 del CPDH mediante el empleo de servicios de inteligencia extranjeros

Según se ha señalado detalladamente más arriba, los Estados contractuales deben cumplir diferentes premisas para que las actividades de sus servicios de inteligencia sean compatibles con

[106] TEDH, Leander, 26.3.1987, apartado 59, Sunday Times, 26.4.1979, apartado 46 y siguientes.
[107] TEDH, Silver y otros, 24.10.1983, apartado 97.
[108] TEDH, Leander, 26.3.1987, apartado 60.
[109] El ponente tiene conocimiento de que Luxemburgo e Irlanda no disponen de un servicio de inteligencia exterior y que tampoco practican ningún SIGINT. El criterio de una instancia de control especial se refiere en este caso únicamente a las actividades de los servicios de inteligencia en el interior.
[110] Sobre la situación de los controles de los servicios de inteligencia en los Estados miembros, véase el capítulo 9.
[111] Cf. al respecto el proyecto de ley "Proposition de loi tendant à la creation de délégations parlementaires pour le renseignement", y el informe a este respecto del diputado Arthur Paecht, nº 1951 Asamblea nacional, 11º período de legislatura, registrado el 23 de noviembre de 1999.

el apartado 8 del CPDH. Es evidente que los servicios de inteligencia no pueden liberarse de estas obligaciones recurriendo a la actividad de otros servicios de inteligencia, que estén sujetos a normas menos severas. En tal caso, el principio jurídico con su doble componente de accesibilidad y flexibilidad perdería su eficacia y se socavaría la jurisprudencia del TEDH en su contenido.

Esto significa, por una parte, que el intercambio de datos entre los servicios de inteligencia sólo es admisible limitadamente. Un servicio de inteligencia únicamente puede recibir datos de otro, cuando éste haya actuado con arreglo a las condiciones previstas en su propio Derecho nacional. El radio de acción previsto en la legislación no puede ampliarse mediante acuerdos con otros servicios. De igual manera, únicamente podrá llevar a cabo actividades para un servicio de inteligencia extranjero de acuerdo con sus instrucciones cuando haya comprobado su conformidad con el propio Derecho nacional. Aun cuando las informaciones estén destinadas a otro Estado, esto no altera la ilegalidad básica de una injerencia imprevista para el sujeto pasivo de derecho.

Por otra parte, los Estados contractuales del CPDH no pueden permitir que los servicios de inteligencia extranjeros actúen en su territorio cuando haya motivos para pensar que su actividad no se ajusta a los criterios del CPDH[112].

8.4.2. Consecuencias para la actividad tolerada de los servicios de inteligencia no europeos en el territorio de Estados miembros del CPDH

8.4.2.1. La jurisprudencia pertinente del Tribunal Europeo de Derechos Humanos

Al ratificar el CPDH, los Estados contractuales se han comprometido a someter el ejercicio de su soberanía al examen de los derechos fundamentales. No pueden cumplir tal obligación renunciando a su soberanía. Los Estados son competentes para su territorio y, por consiguiente, son responsables con respecto a los ciudadanos sujetos al Derecho europeo, incluso cuando el ejercicio del Derecho de soberanía lo asuman los servicios de inteligencia de otro Estado. El TEDH ya ha sentenciado en firme la obligación de los Estados contractuales de adoptar medidas positivas para proteger la esfera privada, para evitar la violación del artículo 8 del CPDH por personas privadas (!), es decir, incluso a nivel horizontal, donde el particular no se enfrenta al poder estatal sino a otra persona[113]. Si un Estado permite a un servicio extranjero actuar en su territorio, la necesidad de proteger es aún mayor, ya que aquí es otra autoridad la que ejerce su soberanía. En tal caso, resulta lógico suponer que el Estado deberá controlar que la actividad de los servicios de inteligencia en su territorio se adecúe a los derechos humanos.

8.4.2.2. Consecuencias para las estaciones

En Alemania se facilita a los Estados Unidos de América en Bad Aibling territorio propio para utilizarlo exclusivamente para la recepción de comunicaciones por satélite. En Menwith Hill, en el Reino Unido, se permite la coutilización de territorio con el mismo objetivo. En caso de que en estas estaciones los servicios de inteligencia norteamericanos intercepten comunicaciones no

[112] Cf. al respecto también Yernault, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, pp. 187 ss.
[113] TEDH, Abdulaziz, Cabales y Balkandali, 28.5.1985, apartado 67; X e Y/Niederlande, 26.3.1985, apartado 23; Gaskin vs Vereinigtes Königreich 7.7.1989, apartado 38; Powell und Rayner, 21.2.1990, apartado 41.

militares de particulares o empresas pertenecientes a un Estado contractual del CPDH, esto conlleva un derecho de supervisión con arreglo al TEDH. Esto significa, en la práctica, que Alemania y Reino Unido, en cuanto Estados contractuales del CPDH, están obligados a cerciorarse de que la actividad de los servicios de inteligencia norteamericanos cumplen los derechos fundamentales. Esto adquiere particular importancia, si se considera que representantes de ONG y de la prensa ya han manifestado en diferentes ocasiones su preocupación por las actividades de la NSA.

8.4.2.3. Consecuencias para las escuchas realizadas por encargo de un tercero

En Morwenstow, en el Reino Unido, de acuerdo con las informaciones con que se cuenta, el GCHQ en colaboración con la NSA intercepta comunicaciones civiles estrictamente con arreglo a sus instrucciones y las entrega como material en bruto a los EE. UU. También en el caso de los encargos para terceros existe la obligación de examinar la conformidad del encargo con los derechos fundamentales.

8.4.2.4. Especial obligación de diligencia en los terceros países

En el caso de los Estados contractuales del CPDH puede suponerse hasta un cierto grado que todos cumplen los principios de dicho Convenio. Se puede partir de tal principio hasta que se demuestre que un Estado contractual del CPDH ha violado sistemática y continuamente dicho Convenio. En el caso de los EE. UU. se trata de un Estado que no es parte contractual del CPDH, y que tampoco se ha sometido a un sistema de control comparable. La actividad de sus servicios de inteligencia está reglamentada muy exactamente, en la medida en que se trate de ciudadanos norteamericanos, es decir, personas que residen legalmente en los EE. UU. Las actividades de la NSA en el extranjero se rigen por otras normas, siendo muchas de ellas confidenciales y, por consiguiente, inaccesibles. Resulta particularmente preocupante que el servicio americano de inteligencia esté sometido al control de las comisiones del Congreso y del Senado, pero que dichas comisiones parlamentarias apenas muestren interés por las actividades de la NSA en el extranjero.

Parece adecuado, por consiguiente, pedir a Alemania y al Reino Unido que se tomen en serio las obligaciones emanadas del CPDH y que permitan la prosecución de las actividades de inteligencia de la NSA en su territorio únicamente cuando éstas se ajusten a lo establecido en el CPDH. A este respecto, deben tenerse en cuenta tres aspectos fundamentales.

1. De conformidad con el CPDH, las injerencias en la vida privada únicamente pueden realizarse con arreglo a normas jurídicas de acceso general y cuyas consecuencias sean previsibles para el particular. Este criterio únicamente se cumplirá cuando los EE. UU. expongan claramente a la población europea de qué manera y bajo qué condiciones realizan sus actividades. En caso de que haya discrepancias con el CPDH, tales normas deberán ajustarse al nivel europeo de protección.

2. De conformidad con el CPDH, las injerencias no deben ser desproporcionadas, y además debe elegirse el medio menos agresivo. Para el ciudadano europeo la injerencia por parte europea se considera menos agresiva que la injerencia americana, ya que únicamente en el primero de estos casos tiene derecho a recurrir a los tribunales nacionales[114]. Las injerencias, por consiguiente,

[114] De esta manera también se logrará la conformidad con el artículo 13 del CPDH, que reconoce al damnificado el

deberán realizarse en la medida de lo posible por parte alemana o británica, lógicamente únicamente con vistas a perseguir delitos. Los norteamericanos han intentado en reiteradas ocasiones justificar la interceptación de las telecomunicaciones con acusaciones de corrupción y soborno por parte europea[115]. Es conveniente indicar a los EE. UU. que todos los Estados de la UE disponen de sistemas operativos de Derecho penal. En caso de que existan indicios de delito, los EE. UU. deberán dejar que sea el país de acogida quien realice las acciones policiales. En caso de que no existan indicios, la vigilancia resulta desproporcionada, por consiguiente, no conforme con los derechos humanos y, por lo tanto, ilegal. Únicamente se produce la conformidad con el CPDH cuando los EE. UU. se limiten a medidas de vigilancia al servicio de su seguridad nacional, y abandonen la persecución de delitos.

3. Según se ha señalado ya, el TEDH ha establecido en su jurisprudencia que para que exista conformidad con los derechos fundamentales debe haber suficientes sistemas de control y garantías contra los abusos. Esto significa que la vigilancia norteamericana de las telecomunicaciones efectuada en territorio europeo únicamente se ajustarán a las normas sobre los derechos humanos cuando los EE. UU. en los casos en que desde dichas ubicaciones intercepten comunicaciones destinadas a proteger su seguridad nacional, prevean controles eficaces al respecto o cuando la NSA someta su actividad en territorio europeo a los organismos de control del país de acogida (es decir, Alemania o el Reino Unido).

Únicamente cuando se cumplan los criterios enumerados en estos tres puntos, podrá asegurarse la conformidad de la actividad de los EE. UU. en la interceptación de telecomunicaciones con el CPDH, de tal manera que éste permita mantener en Europa un nivel de protección unitario garantizado.

---

derecho a presentar recurso ante las instancias nacionales.

[115] Woolsey (ex Director de la CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, p. 31.

9. ¿Están suficientemente protegidos los ciudadanos de la UE con respecto a la actividad de los servicios de inteligencia?

9.1. Protección contra la actividad de los servicios de inteligencia: una tarea de los Parlamentos nacionales

Puesto que en el futuro la actividad de los servicios de inteligencia podría constituir un aspecto de la PESC, pero en la actualidad a escala de la UE no existen normas a este respecto[116], la estructuración de la protección contra la actividad de los servicios de inteligencia depende únicamente de los ordenamientos jurídicos nacionales.

Los Parlamentos nacionales desempeñan a este respecto una doble función: en cuanto órganos legislativos, deciden sobre la existencia y las competencias de los servicios de inteligencia así como sobre la arquitectura del control de la actividad de los servicios de inteligencia. Según se ha expuesto exhaustivamente en el capítulo anterior, los Parlamentos deben supeditarse a la norma relativa a la admisibilidad de la interceptación de las comunicaciones con las limitaciones impuestas por el artículo 8 del CPDH, es decir, que las normas deben ser necesarias, proporcionadas y sus consecuencias previsibles para el particular y que, además, deberán crearse mecanismos de control eficaces y adecuados sobre las competencias de las autoridades de supervisión.

Además, los Parlamentos nacionales desempeñan en la mayoría de los Estados un activo cometido como órganos de control, ya que el control del Ejecutivo (y, por consiguiente, también de los servicios de inteligencia) constituyen, junto con la actividad legislativa, la segunda función "clásica" del Parlamento. Tal arquitectura, sin embargo, difiere en gran manera en los diferentes Estados miembros de la UE, donde, con frecuencia, coexisten órganos parlamentarios y no parlamentarios.

9.2. La competencia de las autoridades nacionales para la ejecución de medidas de vigilancia

La autoridad estatal, por lo general, puede adoptar medidas de vigilancia en materia de persecución penal, para preservar la paz y el orden interior y proteger la seguridad del Estado[117] (con respecto al extranjero).

Con fines de persecución penal en todos los Estados miembros es posible vulnerar el secreto de las comunicaciones, en la medida en que existan indicios suficientes de que una persona concreta ha cometido (a veces, muy cualificado, es decir, con un alto grado de inseguridad). Debido a la gravedad de la injerencia, se precisa para ello, en la regla, una autorización judicial[118]. Hay criterios precisos sobre la duración admisible de la vigilancia, su control y la destrucción de los

[116] Cf. al respecto también el capítulo 7.
[117] Estos fines también los reconoce el apartado 2 del artículo 8 del CPDH como motivos para interferir en la esfera privada. Cf. al respecto el apartado superior 8.3.2.
[118] No es así en el Derecho británico, que comunica la decisión mediante autorización del Secretario de Estado (Regulation of Investigatory Powers Act 2000, Section 5 (1) und (3) (b).

datos.

Para garantizar la seguridad y el orden interior la adquisición estatal de información se amplía más allá de las investigaciones individuales en caso de indicios concretos de delito. A fin de reconocer anticipadamente los movimientos extremistas o subversivos, terroristas o de delincuencia organizada, la legislación nacional permite obtener información adicional sobre determinadas personas o grupos. La recopilación de datos pertinentes, así como su análisis, lo realizan servicios de inteligencia nacionales especiales.

Finalmente, constituyen un importante aspecto de las medidas de vigilancia las que se realizan al servicio de la seguridad estatal. El tratamiento, valoración y comunicación de las informaciones pertinentes sobre el extranjero son competencia, por lo general, de un propio servicio de inteligencia extranjera[119]. El objetivo de la vigilancia no lo constituyen, por lo general, particulares concretos, sino que se investigan más bien determinados ámbitos o frecuencias. Independientemente de los medios con que cuenten los servicios de inteligencia para el extranjero y de sus competencias jurídicas, se trata de un amplio espectro que comprende la investigación meramente militar de la radiodifusión en el ámbito de onda corta hasta la vigilancia de todas formas de telecomunicaciones con el extranjero. En algunos Estados miembros está prohibida la interceptación de las comunicaciones con meros fines de inteligencia[120], en otros Estados miembros -en parte dependiente de la autorización de una comisión independiente[121], por parte de un ministro[122] para ciertas vías de comunicación no existe incluso ningún tipo de limitación[123]. Las competencias comparativamente grandes de ciertos servicios extranjeros de inteligencia se deben a que se dedican a interceptar las comunicaciones extranjeras y, por consiguiente, únicamente afectan a una pequeña porción de los propios sujetos jurídicos pasivos, por lo que existen menores motivos de preocupación.

9.3. El control de los servicios de inteligencia

Resulta particularmente importante, por consiguiente, contar con un control eficaz y global, ya que, por una parte, los servicios de inteligencia trabajan en secreto, sus actividades son a largo plazo y las personas afectadas tampoco se enteran, o no llegan nunca a tener conocimiento de ello, (depende de la situación jurídica) de que han sido objeto de vigilancia y, por otra parte, las medidas de vigilancia afectan con frecuencia a grupos poco definidos de personas, de tal manera que el Estado puede obtener muy rápidamente una gran cantidad de datos personales.

Todos los gremios de control, con plena independencia de su arquitectura, se plantean el problema de que, debido al carácter especial de los servicios secretos, apenas es posible comprobar si realmente se han facilitado todas las informaciones o si se ha retenido una parte de ellas. Esto exige una mayor precisión en materia de reglamentación. Básicamente, puede partirse

[119] Sobre la actividad de los servicios de inteligencia en el extranjero véase la exhaustiva exposición del capítulo 2.
[120] En Austria y Bélgica.
[121] Es el caso de Alemania. Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz). De conformidad con el artículo 9, la Comisión debe ser informada de la intervención (salvo en el caso de peligro inminente).
[122] Es el caso de Gran Bretaña (Regulation of Investigatory Powers Act, Section 1) y de Francia para las comunicaciones de red fija (Art. 3 une 4 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).
[123] Es el caso de las comunicaciones de red fija en Francia (Art. 20 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

de la base de que con una mayor eficacia de control, por consiguiente, se logra una mayor garantía de legalidad de las injerencias cuando la autorización de la vigilancia de las telecomunicaciones es competencia del más alto nivel administrativo, y para su ejecución se precisa una autorización judicial previa y un órgano independiente también controla la puesta en práctica de las medidas. Además, de acuerdo con los principios democráticos, políticos y de Estado de derecho se ajustaran al principio de división de poderes, es decir, estarán sujetos al control de un órgano parlamentario.

Así sucede en gran medida en Alemania. En este país, las medidas de interceptación de las telecomunicaciones las ordena el Ministro federal competente. Salvo en caso de peligro inminente, debe informarse previamente a una comisión independiente, que debe recibir instrucciones ("Comisión G-10"[124]) sobre la admisibilidad y la necesidad de la medida. En los casos en que el servicio de inteligencia para el extranjero BND deba interceptar las telecomunicaciones inalámbricas mediante filtros con conceptos de búsqueda, la Comisión decide también sobre la admisibilidad de tales conceptos de búsqueda. La Comisión G-10, además, es competente para transmitir la comunicación prevista jurídicamente a los afectados, así como para la destrucción de los datos obtenidos por el BND.

Además, existe un gremio de control parlamentario (PKGr)[125] integrado por 9 diputados del Parlamento nacional, que controla la actividad de los tres servicios alemanes de inteligencia. El PKGr tiene derecho a examinar las actas, a interrogar a los colaboradores de los servicios de inteligencia y a visitar sus servicios y a ser informado, si bien esto último puede denegársele cuando así sea necesario debido a razones perentorias de acceso a la información o por razones de protección de los derechos personales de terceras personas o cuando se vea afectado en su propia responsabilidad el núcleo central del ejecutivo. Las deliberaciones del PKGr son secretas, los miembros, también tras haber abandonado su actividad, están obligados a guardar silencio. A comienzos y a finales de la legislatura, el PKGr presenta al Bundestag alemán un informe sobre su actividad de control.

Un control de este tipo, tan amplio, prácticamente sin lagunas, de los servicios de inteligencia es, más bien, la excepción que la regla en los Estados miembros.

En Francia[126], por ejemplo, sólo requieren la autorización del primer ministro las medidas de interceptación que exijan la conexión a una red fija. Sólo éstas están sujetas a la supervisión de una comisión creada a tal efecto (Commission nationale de contrôle des interceptions de sécurité), de la que forman parte un diputado y un senador. La autorización de una medida de escucha solicitada por un ministro o su delegado se transmite al presidente de la Comisión, que en caso de dudar de la legalidad pide a la Comisión que examine la cuestión y ofrezca una recomendación y, en caso de que se sospeche que se produce una violación del Código Penal, informa a la Fiscalía.

Las medidas de escucha con fines de defensa nacional, que comprenden la interceptación de la

[124] Cf. al respecto exhaustivamente: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, Situación a 9.9.2000, editado por el Bundestag alemán, secretaría del PKGr.
[125] Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17 de junio de 1999 BGBl I 1334 idgF.
[126] Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des telécommunications.

radiodifusión, es decir, de las comunicaciones también por satélite, no están sujetas a ningún tipo de limitación y, por consiguiente, tampoco al control de una comisión.

Las actividades de los servicios franceses de inteligencia, además, tampoco están sujetas al control de una comisión de control parlamentario específica, si bien se están sentando ya las bases al respecto. La Comisión de Defensa de la Asamblea Nacional ya ha aprobado una propuesta al respecto[127], pero no se ha celebrado todavía un debate al respecto en sesión plenaria.

En el Reino Unido, toda interceptación de las comunicaciones en suelo británico precisa la autorización de un ministro (Secretario de Estado). La formulación de la ley, sin embargo, no precisa si la interceptación focalizada, amplia de comunicaciones, mediante conceptos clave también estaría sujeta al "Regulation of Investigatory Powers Act 2000" (RIP) y al concepto de "interceptación" previsto en este último, cuando la valoración no se realice en territorio británico, sino que el "material bruto" se transmita sin valoración al extranjero. El control del cumplimiento de las disposiciones del RIP 2000 (con posterioridad) es tarea de un comisionado, un juez del Tribunal Supremo en activo o jubilado designado por el Primer ministro. El comisionado competente para las medidas de interceptación (Interception Commissioner) supervisa la concesión de autorizaciones de escucha y apoya la investigación de las quejas sobre las medidas de vigilancia. El comisionado del Servicio de Inteligencia supervisa las autorizaciones para las actividades de los servicios de inteligencia y seguridad y apoya la investigación de las quejas sobre dichos servicios. El Tribunal de Poderes de Investigación, presidido por un juez superior, examina todas las quejas sobre las medidas de escucha y las actividades de los servicios.

El control parlamentario es tarea de la Comisión de inteligencia y seguridad (ISC)[128], que supervisa la actividad de los tres servicios civiles de inteligencia (M15, M16 y JCHQ). Es competente, en particular, para examinar los gastos y la administración, así como el control de la actividad de los servicios de seguridad, de los servicios de inteligencia y del JCHQ. La comisión está integrada por 9 miembros de la cámara baja y de la cámara alta, entre los que no puede encontrarse ningún ministro. A diferencia de las comisiones de control de otros Estados, que, por lo general, son elegidos o designados por el Parlamento o el presidente del Parlamento, sus miembros son designados por el Primer ministro tras consultar con el líder de la oposición.

Los ejemplos aducidos demuestran ya que el nivel de protección es muy diferente. En lo relativo al control parlamentario, el ponente desea indicar que es muy importante la existencia de una comisión de control que supervise a los servicios de inteligencia. Su ventaja frente a las diferentes comisiones especializadas normales es que disfrutan de una mayor confianza entre los servicios de inteligencia, ya que sus miembros están obligados a guardar secretos y sus reuniones se celebran a puerta cerrada. Además, disponen competencias especiales para cumplir esta tarea especial, lo que resulta fundamental para supervisar las actividades en el sector de los servicios secretos.

Afortunadamente, la mayoría de los Estados miembros de la UE han creado comisiones parlamentarias de control propias para supervisar la actividad de los servicios de inteligencia. En

[127] Cf. al respecto el proyecto de ley "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", y el informe al respecto del diputado Arthur Paecht, nº 1951, Asamblea nacional, 11º período de legislatura, registrado el 23 de noviembre de 1999.
[128] Intelligence services act 1994, Section 10.

Bélgica[129], Dinamarca[130], Alemania[131], Italia[132], los Países Bajos[133] y Portugal[134] existe una comisión de control parlamentaria, que es competente tanto para el control de los servicios de inteligencia civiles como militares. En el Reino Unido[135], supervisa la comisión especial de control sólo la actividad (de hecho, más importante), de los servicios civiles de inteligencia, la actividad de los servicios de inteligencia militares la supervisa la comisión especializada de Defensa. En Austria[136], las dos ramas de los servicios de inteligencia las supervisan dos diferentes comisiones de control, que, de hecho, tienen la misma organización y disfrutan de las mismas competencias. En los Estados escandinavos Finlandia[137] y Suecia[138], son los Defensores del Pueblo los que asumen las tareas del control parlamentario, siendo elegidos por el Parlamento. En Francia, Grecia, Irlanda, Luxemburgo y España, no existen comisiones parlamentarias específicas, las tareas de control se realizan en este ámbito en las comisiones normales especializadas dentro del marco de la actividad parlamentaria general.

9.4. Evaluación de la situación para los ciudadanos europeos

La situación en Europa parece ser poco satisfactoria para los ciudadanos europeos. Las competencias de los servicios de inteligencia en el ámbito de la interceptación de las comunicaciones son muy diferentes en lo relativo a su alcance, y lo mismo es aplicable a las condiciones de control. No todos los Estados miembros que cuentan con un servicio de inteligencia disponen de una comisión parlamentaria de control independiente dotada de las competencias correspondientes de control. Se está muy lejos de poseer un nivel de protección unitario.

Desde la perspectiva europea esto resulta aún más lamentable, ya que esta situación no afecta tanto a los propios ciudadanos de estos Estados, que pueden influir sobre el nivel de protección mediante su opción de voto electoral. Las repercusiones negativas afectan, en particular, a los ciudadanos de otros Estados, ya que el ámbito de actividad de los servicios de inteligencia para el extranjero, naturalmente, se dirigen a éste. El particular está relativamente indefenso frente a

[129] Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 /IV, organique du contrôle des services de police et de renseignements.
[130] Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.
[131] Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.
[132] Comitato parlamentare, L. 24 ottobre 1977, n. 801, Art. 11, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.
[133] Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22.
[134] Conselho de Fiscalização dos Serviços de Informações (CFSI), Ley 30/84 de 5 de septiembre de 1984, modificada por la ley 4/95 de 21 de febrero de 1995, la ley 15/96 de 30 de abril de 1996 y la ley 75-A/97 de 22 de julio de 1997.
[135] Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.
[136] Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung und Ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, Art. 52a B-VG, §§ 32b ff Geschäftsordnungsgesetz 1975.
[137] Defensor del Pueblo, base jurídica para el control de la policía (SUPO): Poliisilaki 493/1995 §33 und Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, para el ámbito militar: Poliisilaki 493/1995 §33 und Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.
[138] Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (Verordnung (1989:773) sobre la autoridad nacional de Policía).

los sistemas extranjeros, siendo la necesidad de protección mucho mayor en este ámbito. Tampoco conviene olvidar que, debido al carácter particular de los servicios de inteligencia, los ciudadanos de la UE se ven afectados por la actividad de diferentes servicios de inteligencia. Sería deseable contar a este respecto con un nivel de protección unitario, que se ajuste a los principios democráticos. En este contexto, debería examinarse en qué medida podrían ponerse en práctica a escala de la UE disposiciones sobre la protección de datos.

Además, la cuestión de la protección del ciudadano europeo adquiere una nueva dimensión si se examina en el marco de una política común de seguridad que conlleve la colaboración de los servicios de inteligencia de los Estados miembros. En tal caso, las instituciones europeas deberán aprobar normas adecuadas de protección. Será tarea del Parlamento Europeo, en cuanto paladín de los principios democráticos, insistir en que sea él quien realice el control correspondiente en cuanto órgano democráticamente legitimado. El Parlamento Europeo también está llamado a establecer las premisas que permitan garantizar el examen confidencial de datos tan sensibles, así como de otros documentos secretos mediante una comisión especialmente configurada, cuyos miembros estén obligados a guardar secreto. Únicamente si se cumplen estas condiciones será realista exigir tales competencias de control con vistas a una colaboración operativa de los servicios de inteligencia, lo que resulta absolutamente imprescindible para una política de seguridad común.

10. La protección contra el espionaje económico

10.1. La economía como objeto de espionaje

En las empresas económicas existen, con vistas a la confidencialidad, tres tipos de informaciones. Por una parte, están las informaciones que intencionalmente **deben adquirir la mayor difusión**. Se trata, por ejemplo, de las informaciones sobre los productos de la empresa (por ejemplo, cualidades del producto, precios, etc.) e informaciones publicitarias, que influyen sobre la imagen de la empresa.

Existen también informaciones que **no se protegen ni se difunden activamente**, porque tienen poco que ver con la posición competitiva de la empresa. Por ejemplo, la fecha de la excursión de la empresa, el menú de la cantina o la marca de los aparatos de fax utilizados.

Y, finalmente, están las informaciones que **deben protegerse del conocimiento de terceros**. Tales informaciones se protegen frente a la competencia, incluso, si la empresa no desea cumplir la ley, por el Estado (impuestos, normativas sobre el embargo, etc.). Existen a este respecto diferentes tipos de protección, que llegan hasta el secreto absoluto como, por ejemplo, los resultados de la investigación antes de la comunicación de las patentes o en la producción de bienes de defensa[139].

El espionaje, en el caso que se examina actualmente, se refiere a la adquisición de las informaciones que mantiene en secreto una empresa. Cuando el agresor es una empresa de la competencia, se habla de **espionaje competitivo** (también espionaje industrial, espionaje laboral). Cuando el agresor es un servicio de inteligencia estatal, se habla de **espionaje económico**.

10.1.1. Los objetivos del espionaje en detalle

Los datos estratégicos, que son importantes para el espionaje destinado al sector económico, se pueden clasificar por sectores o sectores empresariales.

10.1.1.1. Sectores

Es evidente que tienen gran interés las informaciones de los siguientes sectores: biotecnología, ingeniería genética, técnica medicinal, técnica ambiental, ordenadores de alto rendimiento, aplicaciones informáticas, optoelectrónica, tecnología de señales y sensores ópticos, memorias electrónicas, cerámica técnica, aleaciones de alto rendimiento y nanotecnología. La lista no es completa y, además, cambia constantemente de acuerdo con el desarrollo tecnológico. En estos ámbitos, el espionaje consiste, sobre todo, en robar los resultados de la investigación o técnicas especiales de producción.

10.1.1.2. Sectores empresariales

Los objetivos de los ataques de espionaje se encuentran, lógicamente, en los sectores de investigación y desarrollo, adquisiciones, personal, producción, distribución, ventas,

[139] Informaciones para las empresas sujetas a la protección secreta, BMWI 1997.

comercialización, líneas de productos y finanzas. Con frecuencia se infravalora la importancia y el valor de tales datos (véase más abajo 10.1.4.).

10.1.2. Espionaje competitivo

La posición estratégica de una empresa en el mercado depende de su estado en los ámbitos de la investigación y desarrollo, métodos de producción, líneas de producción, financiación, comercialización, venta, distribución, adquisiciones y mano de obra[140]. Las informaciones al respecto son muy interesantes para todo competidor en el mercado, ya que desvelan los planes y debilidades, así que es posible elaborar medidas estratégicas de contraataque.

Una parte de tales informaciones es de acceso público. Existen empresas consultoras muy especializadas, que dentro de un marco plenamente legal elaboran un análisis de competencia, como, por ejemplo, empresas de tan gran renombre como Roland & Berger en Alemania. "Competitive Intelligence" es en los Estados Unidos, entretanto, una herramienta estándar de gestión[141]. De una pluralidad de pequeñas informaciones es posible elaborar una clara imagen de la situación mediante un tratamiento profesional.

La transición de legalidad a espionaje industrial ilegítimo se basa en la elección de los medios con los que se obtiene la información. Tan sólo cuando los medios empleados son ilegales en el marco jurídico correspondiente, comienza a ser delictiva la actividad -la realización de análisis no es en sí delictiva-. Las informaciones particularmente interesantes para los competidores, naturalmente, son confidenciales y únicamente pueden obtenerse violando la ley. Las técnicas empleadas al respecto no se diferencian en nada de los métodos generales de espionaje descritos en el capítulo 2.

No se cuenta con informaciones precisas sobre las dimensiones del espionaje competitivo. Las cifras sumergidas, al igual que en el espionaje clásico, son muy altas. Ambas partes interesadas (agresor y víctima) no están interesadas en la publicidad. Para las empresas afectadas esto siempre supone una pérdida de imagen y los agresores, naturalmente, no tienen ningún interés en publicar sus actividades. Por consiguiente, únicamente se presentan pocos casos ante los tribunales.

Sin embargo, con frecuencia se informa en la prensa sobre el espionaje competitivo. El ponente ha hablado a este respecto con algunos jefes de seguridad de grandes empresas alemanas[142] y con ejecutivos de empresas americanas y europeas. En resumen, puede constatarse que el espionaje competitivo siempre se descubre, pero que no determina la actividad cotidiana.

10.2. Los daños originados por el espionaje económico

Debido a la gran cifra sumergida, no puede cifrarse exactamente la dimensión de los daños que causa el espionaje competitivo o económico. Además, una parte de las cifras citadas son interesadas. Las empresas de seguridad y los servicios de contraespionaje tienen un interés comprensible de elevar al extremo superior de lo posible el daño causado por el espionaje. Sin embargo, las cifras ofrecen una cierta impresión.

[140] M.F.Porter, Competitive Strategy.
[141] Hummelt, Roman, espionaje económico en la autopista de la información, Hanserverlag, Munich 1997.
[142] No se mencionan los detalles ni los nombres.

En 1988, el Instituto Max Planck ya cifraba los daños originados por el espionaje económico en Alemania en al menos 8 000 millones de marcos[143]. El presidente de la asociación de empresas de seguridad en Alemania cita, remitiéndose a expertos, una cifra de 15 000 millones de marcos anualmente. El Presidente del Sindicato Europeo de Policía, Hermann Lutz, evalúa los daños en 20 000 millones de dólares anualmente. El FBI[144] calcula para los años 1992/1993 unas pérdidas de 1 700 millones de dólares, que ha sufrido la economía norteamericana mediante el espionaje en materia de competencia industrial. El expresidente de la Comisión de control de los servicios secretos del congreso de los EE. UU. habla de 100 000 millones de dólares norteamericanos en pérdidas, debido a la pérdida de encargos y a los costes adicionales de investigación y desarrollo. Entre 1990 y 1996 esto ha tenido como consecuencia la pérdida de 6 millones de puestos de trabajo[145].

En principio, no es necesario conocer exactamente los daños. El Estado está obligado, junto con la Policía y las autoridades de contraespionaje a actuar independientemente contra el espionaje económico y competitivo, independientemente del importe de las pérdidas para la economía nacional. Las cifras de pérdidas totales no son una base adecuada para las decisiones que deben adoptar las empresas sobre la protección de las informaciones y las propias medidas de contraespionaje. Toda empresa debe procurar evaluar el máximo daño posible que puede producir el robo de información, la posibilidad de que éste se produzca y, por consiguiente, las cifras que esto conlleve en compensación con los costes de la seguridad. El problema principal no lo constituye la falta de cifras globales exactas. El problema es más bien que, aparte de en las grandes empresas, no se realiza ningún tipo de cálculos coste/utilidad y, por consiguiente, se descuida la seguridad.

10.3. ¿Quién espía?

Los principales clientes del espionaje contra empresas se describen en un estudio de la empresa de auditoría económica Ernest Young LLP[146], llevado a cabo con 39 competidores, 19 clientes, 9 suministradores y 7 servicios secretos. Realizan tareas de espionaje los propios empleados, las empresas privadas de espionaje, los piratas informáticos a sueldo y los profesionales de los servicios secretos[147].

10.3.1. Propios empleados (delitos internos)

La evaluación de la literatura especializada, las informaciones a este respecto de los expertos en comisión y las conversaciones mantenidas por el ponente con jefes de seguridad y autoridades de espionajes coinciden en demostrar lo siguiente: el mayor peligro de espionaje parte de unos empleados desilusionados e insatisfechos. En cuanto empleados de la empresa tienen acceso directo a las informaciones, se venden por dinero y averiguan para sus clientes los secretos de la empresa.

También conlleva grandes riesgos el cambio de empleo. Hoy en día no es necesario copiar

[143] IMPULSE,3/97,S.13 ff.
[144] Congressional Statement, L.J.Freech, Director FBI, 9.5.1996.
[145] Robert Lyle, Radio Liberty/Radio fre Europe, 10 de febrero de 1999.
[146] Computerzeitung, 30.11.1995, p. 2.
[147] R.Hummelt, Spionage auf dem Datenhighway, München 1997, p. 49 y ss.

montañas de papeles para llevarse informaciones de una empresa. Éstas se pueden archivar discretamente en disquetes y llevarse a la nueva empresa cuando se cambie de empleo.

10.3.2. Empresas privadas de espionaje

El número de empresas que se ha especializado en la búsqueda de datos crece continuamente. En parte, trabajan en tales empresas antiguos empleados de los servicios de inteligencia. Estas empresas trabajan frecuentemente tanto como empresas asesoras en materia de seguridad como agencias de detectives que obtienen informaciones por encargo. Como norma general se utilizan métodos legales, pero también hay empresas que emplean métodos ilegales.

10.3.3. Piratas informáticos

Los piratas informáticos son especialistas en ordenador que con sus conocimientos obtienen desde el exterior acceso a las redes de ordenadores. En los años iniciales, los piratas informáticos eran chiflados de la informática a los que les divertía superar las barreras de seguridad de los sistemas de ordenadores. En la actualidad, hay piratas informáticos que trabajan por encargo, tanto para los servicios de inteligencia como para el mercado.

10.3.4. Servicios de información

Después de finalizada la guerra fría, las tareas de los servicios de inteligencia se han desplazado. La delincuencia internacional organizada y la situación económica son sus nuevos ámbitos de actividad (véase más al respecto en el capítulo 10, 10.5.).

10.4. ¿Cómo se espía?

De acuerdo con las informaciones de las autoridades de contraespionaje y los jefes de seguridad de las grandes empresas, en el espionaje económico se emplean todos los métodos e instrumentos acreditados en los servicios de inteligencia (véase el capítulo 2, 2.4.). Las empresas tienen unas estructuras más abiertas que los organismos militares y los servicios de inteligencia o los órganos gubernamentales. El espionaje económico supone, por consiguiente, riesgos adicionales:

- el reclutamiento de empleados es sencillo, porque las posibilidades en la seguridad de las empresas no es comparable a la de las autoridades de contraespionaje;

- la movilidad laboral hace que importantes informaciones se lleven en el ordenador portátil. El robo de ordenadores portátiles o la copia secreta del disco duro tras el acceso ilegal a la habitación del hotel forman parte del sistema estándar del espionaje industrial;

- el acceso a las redes informáticas es más sencillo que en las instituciones estatales con mayor sentido de la seguridad, porque precisamente en las pequeñas y medianas empresas están menos desarrollados los mecanismos y conciencia de la seguridad;

- las escuchas sobre el terreno (véase el capítulo 3, 3.2.) son más sencillas por los mismos motivos.

La evaluación de las informaciones recopiladas permite deducir que el espionaje económico se realiza fundamentalmente sobre el terreno o en un lugar de trabajo móvil, pues con pocas excepciones (véase más abajo 10.6.) la información deseada no se consigue mediante la interceptación de las redes internacionales de telecomunicaciones.

10.5. Espionaje económico realizado por los Estados

10.5.1. Espionaje económico estratégico por parte de los servicios de inteligencia

Una vez finalizada la guerra fría, se han liberado capacidades en los servicios de inteligencia que ahora se emplean en otros ámbitos. Los EE. UU. indican claramente que una parte de las actividades de sus servicios de inteligencia se basa en la industria. Entre otras actividades, realizan, por ejemplo, la vigilancia del mantenimiento de las sanciones económicas, la vigilancia del cumplimiento de las normas para el suministro de armas y de los llamados productos de doble uso, las tendencias en los mercados de materias primas y el desarrollo de los mercados financieros internacionales. Según ha tenido conocimiento el ponente, no son únicamente los servicios de los EE. UU. los que actúan en este ámbito y tampoco hay grandes críticas al respecto.

10.5.2. Servicios de inteligencia como agentes de espionaje competitivo

Se formulan críticas cuando los servicios estatales de inteligencia se emplean inadecuadamente para conseguir que las empresas de su territorio estatal mediante el espionaje detengan ventajas en la competencia internacional. A este respecto, es preciso diferenciar dos aspectos[148].

10.5.2.1. Estados de alta tecnología

Los Estados industriales muy desarrollados pueden beneficiarse plenamente del espionaje industrial. Mediante el estudio del grado de desarrollo de un sector pueden ponerse en marcha medidas extraeconómicas y acciones políticas subvencionadas que hacen que la propia industria sea más competitiva o se puedan ahorrar subvenciones. Otro aspecto central lo constituye la obtención de detalles en el caso de licitaciones con un gran valor contractual (véase más abajo 10.6.).

10.5.2.2. Estados menos avanzados tecnológicamente

Una parte de estos Estados se esfuerza por obtener conocimientos técnicos para superar el atraso de la propia industria o reducir los costes de desarrollo y los cánones por licencia. Además, se trata también de obtener muestras y técnicas de producción para ser más competitivos en el mercado mundial con productos copiados y más baratos (menores salarios). Está demostrado que los servicios rusos han recibido tal encargo. La Ley federal nº 5 de la Federación de Rusia sobre las actividades de los servicios de inteligencia en el extranjero citan expresamente la obtención de informaciones económicas y científico-tecnológicas como tarea de los servicios de

[148] Investigación privada de un servicio de contraespionaje al ponente. Fuente protegida.

inteligencia.

Para otros Estados (por ejemplo, Irán, Iraq, Siria, Libia, Corea del Norte, India y Paquistán), se trata sobre todo de obtener informaciones para sus programas nacionales de defensa, en particular, en el ámbito nuclear y en el ámbito de las armas químicas y biológicas. Otro aspecto de la actividad de los servicios de estos Estados es crear empresas fantasmas que compren productos de doble uso de manera poco sospechosa.

10.6. ¿Es adecuado ECHELON para el espionaje industrial?

Con el control estratégico del tráfico internacional de telecomunicaciones únicamente pueden obtenerse informaciones importantes para el espionaje competitivo por casualidad. De hecho, las informaciones sensibles de las empresas se encuentran, sobre todo, en las propias empresas, **por lo que el espionaje competitivo, en primera línea, tiene por objetivo obtener** informaciones **mediante empleados** o personas infiltradas o introducirse en las redes informáticas internas. Únicamente cuando las informaciones sensibles se transmiten al exterior mediante redes fijas o radiodifusión (satélite), puede emplearse un sistema de interceptación de las comunicaciones para el espionaje competitivo. Esto ocurre sistemáticamente en los siguientes tres casos:

- en empresas que trabajan en tres zonas horarias, por lo que los resultados provisionales se envían de Europa a América y, a continuación, a Asia;

- en el caso de las videoconferencias en consorcios multinacionales, que se realizan mediante V-Sat o cable;

- cuando se negocian sobre el terreno importantes contratos (por ejemplo, construcción de instalaciones, mejora de la infraestructura de telecomunicaciones, construcción de nuevo cuño de sistemas de transporte, etc.) y desde ahí deben mantenerse contactos con la central de la empresa.

Cuando las empresas no protegen su comunicación en estos casos, la interceptación de dichas comunicaciones facilita datos valiosos al espionaje industrial.

10.7. Casos publicados

Hay algunos casos de espionaje económico o competitivo que se han publicado en la prensa pública o en la literatura especializada. Una parte de dichas fuentes se ha evaluado y se ha resumido en el siguiente cuadro. Se indica brevemente quién ha intervenido, cuándo se ha producido el caso, de qué se trataba, cuál era el objetivo y qué consecuencias tuvo.

Es curioso que, en parte, se informe de manera muy distinta sobre un mismo caso. Por ejemplo, véase el caso Enercon, en el que se describe como "agresor" a la NSA o al Ministerio de Economía de los EE. UU. o al fotógrafo competidor.

Caso	Quién	Cuándo	Qué	Cómo	Objetivo	Consecuencias	Fuente
Air France	DGSE	Hasta 1994	Conversación de ejecutivos viajeros	En las cabinas de 1ª clase de Air France se descubrieron chinches - la empresa se disculpó públicamente	Obtención de informaciones	Se desconocen	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/
Airbus	NSA	1994	Informaciones sobre negociaciones económicas entre Airbus y una línea aérea de Arabia Saudita	Interceptación de fax y teléfono entre los interlocutores	Transmisión de la información al competidor americano Boeing y Mc Donnell Douglas	Los americanos celebran un contrato de 6 000 millones de dólares	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. noviembre de 2000
Airbus	NSA	1994	Contrato superior a 6 000 millones de dólares con Arabia Saudi Descubrimiento de soborno del consorcio europeo Airbus	Interceptación de fax y teléfono entre el consorcio europeo Airbus y la línea aérea saudí/Gobierno mediante comunicación por satélite	Descubrimiento de soborno	Mc Donnel Douglas, el competidor americano de Airbus, consigue el contrato	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell
BASF	Distribuidor	Se desconoce	Descripción del procedimiento para la producción de la materia prima de la crema cutánea de la empresa BASF (sección de cosmética)	Se desconoce	Se desconoce	Ninguna, porque se descubrió	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16. octubre de 1992
Ministerio federal de economía de Alemania	CIA	1997	Informaciones sobre productos de alta tecnología en el Ministerio federal de economía	Empleo de agentes	Obtención de información	El agente es descubierto y expulsado al ser detectado	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Ministerio federal de economía de Alemania	CIA	1997	Trasfondo del proceso Mykonos des Berliner, créditos Hermes con respecto a las exportaciones a Irán, listado de las empresas alemanas que exportan productos de alta tecnología a Irán	Agente de la CIA camuflado como embajador de los EE.UU. celebra conversaciones amistosas con el jefe del departamento del Ministerio federal de economía competente para el ámbito árabe (en particular, Irán)	Obtención de información	Se desconoce. El funcionario se dirige a los servicios de seguridad alemanes, que indican a las autoridades norteamericanas que la operación de la CIA no es deseable. A continuación, el agente de la CIA es retirado	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Situación a: 1998
Dasa	Russischer NDs	1996 – 1999	Venta y transmisión de documentación sobre tecnología de defensa de una empresa muniquesa de tecnología militar (de acuerdo con el SZ / 30.05.2000: Rüstungskonzern Dasa in Ottobrunn)	2 delegados alemanes	Obtención de información sobre misiles, sistemas de armamento (tanques y defensa antiaérea)	SZ / 30.05.2000: “ (...) Traición bajo el punto de vista militar “no particularmente grave”. Lo mismo es aplicable a los daños económicos, constató el Tribunal.”	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, abril de 2001 „Haftstrafe wegen Spionage für Russland“, SDZ / 30 de mayo de 2000
Embargo	BND	Hacia 1990	Nuevo embargo sobre las exportaciones de las tecnologías protegidas a Libia (entre otros, por Siemens)	Interceptación de las telecomunicaciones	Descubrimiento de una transferencia ilegal de armas y tecnología	Sin consecuencias particulares, no se impidieron los suministros	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 110

Caso	Quién	Cuándo	Qué	Cómo	Objetivo	Consecuencias	Fuente
Enercon	Especialista en tecnología eólica de Oldemburgo y empleada de Kenetech	No se conoce	Generador de energía eólica de la empresa Enercon de Auricher	No se conoce	No se conoce	No se conoce	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, abril de 2001
Enercon	NSA	No se conoce	Molino de viento para la obtención de electricidad, desarrollado por el ingeniero de Frisia oriental Aloys Wobben	No se conoce	Transmisión de los detalles técnicos de Wobbens a la empresa de los Estados Unidos	La empresa estadounidense solicita la patente del molino de viento de Wobben antes que éste; Wobben es acusado por un bufete de abogados de los EE.UU. (violación del derecho de patentes)	„Aktenkrieger“, SZ, 29. marzo de 2001
Enercon	Empresa estadounidense Kenetech Windpower Corp	1994	Importantes detalles de la instalación de alta tecnología eólica (Desde los interruptores hasta las platinas)	Fotografías	Procedimiento de patente con éxito en los EE.UU.	Enercon GmbH proyecta de tener su acceso al mercado americano	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. Agosto de 1996
Enercon	Ingeniero W de Oldenburgo y empresa norteamericana Kenetech	Marzo 1994	Generador eólico del Tipo E-40 de Enercon	El ingeniero W. facilita informaciones, empleada de Kenetech fotografía la instalación más los detalles electrónicos	Kenetech: busca pruebas para una posterior demanda por violación de la patente contra Enercon (1995) Enercon: obtención ilegal de información sobre secretos de empresa Un periodista televisivo parece haber averiguado mediante un exempleado de la NSA que el conocimiento detallado de Enercon se ha transmitido a Kenetech por parte norteamericana mediante Echelon	No se conoce	„Klettern für die Konkurrenz“, SZ 13 de octubre de 2000
Enercon	Kenetech Windpower	Antes de 1996	Instalaciones para la producción de energía eólica de Enercon	Ingenieros de Kenetech fotografían la instalación	Réplica de la instalación en Kenetech	Enercon recibe justicia; se acusa a los espías; pérdidas previstas: varios millones de marcos	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Ministerio de Comercio del Japón	CIA	1996	Negociaciones sobre la cuota de importación para coches norteamericanos del mercado japonés	Piratería informática en sistemas informáticos del ministerio japonés de comercio	El negociador norteamericano Mickey Kantor debe aceptar la oferta más barata	Kantor acepta la oferta más barata	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Coches japoneses	Gobierno de los EE.UU.	No se conoce	Negociaciones sobre la importación de coches japoneses de lujo Información sobre las normas de emisión de los coches japoneses	COMINT, no se describe exactamente	Obtención de informaciones	No se conoce	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell

Caso	Quién	Cuándo	Qué	Cómo	Objetivo	Consecuencias	Fuente
López	NSA	Se desconoce	Videoconferencia de VW y López	Escuchas desde Bad Aibling	Transmisión de la información a General Motors y Opel	Mediante las escuchas la fiscalía tenía "informaciones muy detalladas" para su investigación	Bundeswehrhauptmann Erich Schmidt-Eenboom, zitiert in „Wenn Freunde spionieren“ www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López y tres de sus colaboradores	1992 - 1993	Documentos y datos de los ámbitos de investigación, planificación, construcción y adquisiciones (documentación para la fábrica en España, datos sobre el coste de diferentes series de modelos, estudios de proyectos, estrategias de compra y ahorro)	Recopilación de material	Empleo de la documentación de General Motors por VW	Tras una disputa judicial, los consorcios logran un acuerdo extrajudicial. López dimite en 1996 como ejecutivo de VW. VW despide en 1997 a tres colaboradores más del equipo de López, paga 100 millones de dólares a GM/Opel (al parecer, costes de abogados) y adquiere durante 7 años piezas de repuesto por un importe superior a 1000 millones de dólares de GM/Opel	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Situación a: 1998
López	NSA	1993	Videoconferencia entre José Ignacio López y el jefe de VW Ferdinand Piëch	Grabación de la videoconferencia y transmisión a General Motors (GM)	Protección de los secretos de empresa de la GM norteamericana, que López deseaba facilitar a VW (listas de precios, planes secretos sobre una nueva fábrica de coches y nuevos utilitarios)	López es descubierto, el procedimiento judicial se detiene en 1998 mediante el pago de multas. No se sabe nada con respecto a la NSA	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 de noviembre de 2000 „Abgehört“, Berliner Zeitung, 22 de enero de 1996 „Die Affäre López ist beendet“, Wirtschaftsspiegel, 28 de julio de 1998 „Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Los Álamos	Israel	1988	Dos empleados del programa de investigación atómica de Israel logran entrar en el ordenador central del laboratorio de armas atómicas de Los Álamos	Piratería electrónica	Obtención de información sobre nuevos detonadores de armas atómicas de los EE.UU.	Ninguna consecuencia especial, ya que los piratas informáticos huyen a Israel, uno es detenido allí provisionalmente, oficialmente no se habla de ninguna relación oficial con los servicios secretos de Israel	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 137
Contrabando	BND	Años 70	Contrabando de instalaciones informáticas a la RDA	Se desconoce	Descubrimiento de la transferencia de tecnología al bloque del Este	Sin consecuencias, no se impiden los suministros	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 113

Caso	Quién	Cuándo	Qué	Cómo	Objetivo	Consecuencias	Fuente
TGV	DGSE	1993	Evaluación de costes de Siemens Contrato para suministro de trenes de alta velocidad a Corea del Sur	Se desconoce	Oferta más barata	El fabricante del ICE pierde el contrato en favor de Alcatel - Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
TGV	Se desconoce	1993	Evaluación de costes de AEG y Siemens sobre una licitación pública en Corea del Sur para el suministro de trenes de alta velocidad	Siemens indica que sus comunicaciones telefónicas y de fax han sido interceptadas en su sucursal en Seúl	Ventaja negociadora del competidor británico - francés GEC Alsthom	El cliente opta por GEC Alsthom, aunque la oferta alemana era en principio mejor	„Abgehört“, Berliner Zeitung, 22 de enero de 1996
Thomson-Alcatel contra Raytheon	CIA/NSA	1994	Concesión de un contrato multimillonario brasileño para la vigilancia por satélite del Amazonas a la empresa Thompson-Alcatel (1 400 millones de dólares)	Interceptación de las telecomunicaciones del ganador de la licitación (Thompson-Alcatel, FR)	Descubrimiento de corrupción (pago de sobornos)	Clinton se queja ante el Gobierno brasileño; debido a las presiones del Gobierno de los EE.UU. se concede el contrato a la empresa norteamericana "Raytheon"	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 91
Thomson-Alcatel contra Raytheon	Ministerio de Economía de los EE.UU "se ha esforzado"	1994	Negociaciones sobre un proyecto millonario para la vigilancia por radar del bosque tropical brasileño	Se desconoce	Obtención del contrato	Los consorcios franceses Thompson, CSF y Alcatel pierden en favor de la empresa norteamericana Raytheon el contrato	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. noviembre de 2000
Thomson-Alcatel contra Raytheon	NSA Departamento de Comercio	Depar-tament o de Comer-cio	Negociaciones sobre un proyecto multimillonario (1 400 millones de dólares) para la vigilancia del Amazonas (SIVA) Descubrimiento de sobornos del grupo brasileño de selección Comentario de Campbell: Raytheon mejora la estación de escuchas en Sugar Grove	Escuchas de las negociaciones entre Thompson y CSF y Brasil y transmisión de los resultados a Raytheon Corp.	Descubrimiento de sobornos Celebración del contrato	Raytheon recibe adjudicado el contrato	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Contrato millonario para la estación de gas y petróleo en el Mar del Norte	Interceptación del fax del ganador de la licitación (Thyssen)	Descubrimiento de corrupción	BP demanda a Thyssen para el pago de una compensación	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 92
VW	Se desconoce	"pasan los años"	Se desconoce	Cámaras de infrarrojos enterradas en montículos de tierra con ??? que transmiten imágenes por radio	Obtención de información sobre nuevos descubrimientos	VW admite pérdidas por importe de tres cifras	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. agosto de 1996
VW	Desconocido	1996	Tramo de pruebas en Ehra-Lessien de VW	Cámara oculta	Informaciones sobre nuevos modelos de VW	Se desconoce	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11 de junio de 1998

10.8. Protección contra el espionaje electrónico

10.8.1. Protección jurídica

En los ordenamientos jurídicos de todos los Estados industriales, el robo de secretos de empresa es ilegal. Como en todos los demás casos del Derecho penal, también el nivel de protección nacional resulta muy diferente. En líneas generales, puede afirmarse que la pena prevista es claramente inferior a la de los casos de espionaje en el contexto de la seguridad militar. En numerosas ocasiones, el espionaje competitivo sólo se prohíbe cuando se trata de empresas nacionales, pero no cuando se espía a empresas extrajeras. Este es también el caso de los Estados Unidos de América.

Las leyes pertinentes prohíben, en principio, únicamente las actividades de espionaje de las empresas industriales entre sí. Es cuestionable si limitan también la actividad de todos los servicios de inteligencia, ya que éstos, en virtud de las leyes por las que han sido creados, tienen derecho a robar informaciones.

Se plantea un caso límite cuando los servicios de inteligencia facilitan a las empresas las informaciones obtenidas mediante espionaje. Normalmente, esto ya no se ajustaría a las leyes que conceden competencias especiales a los servicios de inteligencia. En particular, en el caso de la UE, esto supondría una violación del Tratado CEE (véase el capítulo...).

Además, en la práctica, solicitar el amparo jurídico de los tribunales resultaría muy difícil para las empresas. Las escuchas no dejan huellas y no dejan pruebas admisibles en los tribunales.

10.8.2. Obstáculos particulares para el espionaje económico

Los Estados aceptan el hecho de que los servicios de inteligencia para obtener información estratégica general también actúen en el ámbito de la economía. Tal "acuerdo entre caballeros", sin embargo, se viola considerablemente en el espionaje competitivo en favor de la propia industria. Si se logra demostrar que un Estado ha actuado de tal manera, éste se vería enfrentado a graves problemas políticos. Éste sería el caso de una potencia mundial como los EE.UU., cuyo deseo de conseguir una dirección política global se vería espectacularmente perjudicado. Las potencias medianas podrían permitirse más bien ser descubiertas, una potencia mundial, no.

Al margen de los problemas políticos se plantean también las cuestiones prácticas, como, por ejemplo, a qué empresa particular deberían facilitársele los resultados del espionaje competitivo. En el ámbito de la construcción aeronáutica la respuesta es sencilla, porque aquí a escala mundial únicamente hay dos grandes competidores. En todos los demás casos, donde existen diferentes empresas que no son de control estatal, es muy difícil favorecer a una en concreto. En el caso de la transmisión de información detallada sobre las ofertas de competidores a empresas particulares en el contexto de licitaciones públicas internacionales, facilitar las informaciones obtenidas por espionaje a todos los competidores del propio país sería posible. Así se haría, en particular, cuando la estructura de apoyo del Gobierno sea accesible de la misma forma a todos los competidores nacionales, según ocurre en los EE.UU. con el llamado Centro de Interlocución. En el caso del robo de tecnología que conduce

obligatoriamente a la inscripción de una patente, lógicamente ya no sería posible dar el mismo trato a todas las empresas.

Esto supondría, en particular, un gran problema en el sistema político norteamericano. Los políticos norteamericanos dependen en gran medida de las donaciones de la industria en sus circunscripciones electorales para financiar sus campañas electorales. En caso de que se favoreciera obviamente a ciertas empresas mediante los servicios de inteligencia, se producirían grandes alteraciones en el sistema político. Así lo formuló el ex director de la CIA Woolsey en una conversación con representantes de la comisión: "en tal caso la cota (es decir, el congreso de los EE.UU.) se volvería loco" ¡Al que tiene razón hay que dársela!

10.9. Los EE.UU. y el espionaje económico

10.9.1. La posición oficial de los EE.UU. sobre el espionaje económico

El exdirector de la CIA, Woolsey, y el presidente de la Comisión de Control de los Servicios Secretos del Congreso, Porter Goss, han defendido en las conversaciones celebradas, brevemente, las siguientes posiciones:

1. Los EE.UU. interceptan las telecomunicaciones internacionales para obtener información general sobre las tendencias económicas, sobre el suministro de productos de doble uso y el cumplimiento de los embargos.

2. Los EE.UU. interceptan focalizadamente las comunicaciones de empresas particulares en el contexto de licitaciones a fin de impedir distorsiones del mercado mediante soborno en perjuicio de empresas de los Estados Unidos.

El soborno empresarial está jurídicamente prohibido en los EE.UU. y los auditores están obligados a comunicarlo cuando lo descubren. En caso de que la interceptación de las comunicaciones descubriera el soborno en licitaciones públicas, el embajador norteamericano intervendría ante el gobierno del país de que se tratase. Las empresas norteamericanas que también intervinieran en la licitación, por el contrario, no serían informadas directamente.

10.9.2. El cometido del Centro de Interlocución en el fomento de las exportaciones norteamericanas

10.9.2.1. El cometido del Centro de Interlocución

El Centro de Interlocución del Ministerio del Comercio de los EE.UU. es el núcleo de la estrategia nacional de exportación practicada por el presidente Clinton y luego seguida por Bush. El Centro, fundado en 1993, ha ayudado desde entonces a cientos de empresas norteamericanas a obtener contratos públicos en el extranjero. El Centro coordina los diferentes recursos del Gobierno de los EE.UU. desde los conocimientos técnicos en sectores concretos, pasando por el agregado de economía de las embajadas hasta la Casa Blanca.

10.9.2.2. El funcionamiento del Centro

En el propio Centro trabaja únicamente una pequeña plantilla de doce personas (situación a

6.2.2001). El Centro es el principal mediador de las empresas con las diferentes autoridades de la administración de los EE.UU. que se ocupan de promover la exportación. Actúa de manera no discriminatoria para las empresas, apoya, sin embargo de acuerdo con unos claros principios únicamente proyectos de interés nacional de los EE.UU. Por consiguiente, los productos suministrados deben proceder, al menos en un 50% de su valor, de los EE.UU.

10.9.2.3. Cuestiones abiertas en el contexto del Centro

El Gobierno norteamericano no ha permitido que se celebre la conversación prevista entre miembros de la comisión y del Centro. Por consiguiente, no pudieron examinarse dos cuestiones que plantean dudas.

a) la comisión posee documentos que parecen demostrar una participación de la CIA en las actividades del Centro.

b) el Centro facilita en el marco de las informaciones colocadas en Internet, que reúne los recursos de 19 Agencias gubernamentales de los EE.UU. En otro lugar se citan, expresamente, únicamente 14 Agencias. Se plantea la cuestión de por qué no se citan expresamente los nombres de las 5 Agencias restantes.

10.10. La seguridad de las redes informáticas

Se presentará posteriormente

10.11. La infravaloración de los riesgos

Se entregará posteriormente

10.11.1. Grandes empresas

10.11.2. Pequeñas y medianas empresas

10.11.3. Instituciones europeas

10.11.4. Centros de investigación

11. Autoprotección mediante la criptografía

11.1. Objetivo y funcionamiento de la codificación

11.1.1. Objetivo de la codificación

Toda transmisión de información conlleva el riesgo de que caiga en manos de personas no autorizadas. En este caso, si se quiere evitar que terceros accedan a su contenido, hay que adoptar medidas para que el mensaje sea ilegible o imposible de interceptar, es decir, hay que codificarlo. Por esta razón, las técnicas de codificación se utilizan desde tiempo inmemorial en los ámbitos militar y diplomático.[159]

En los últimos 20 años la codificación ha adquirido cada vez mayor importancia, ya que el porcentaje de comunicaciones dirigidas al extranjero, en donde el país desde el que se envían ya no está en condiciones de proteger el secreto de la correspondencia ni de las telecomunicaciones, es cada vez mayor. Asimismo, el incremento de las posibilidades técnicas de las que disponen los Estados para interceptar/grabar legalmente las comunicaciones ha generado una mayor necesidad de protección de parte de los ciudadanos que están preocupados. Además, el interés cada vez mayor que demuestran los delincuentes por acceder ilegalmente a la información y por falsificarla ha dado pie a medidas de protección (por ejemplo, en el sector bancario).

La invención de las comunicaciones eléctricas y electrónicas (telégrafo, teléfono, radio, télex, fax e Internet) ha simplificado enormemente la transmisión de mensajes y la hecho más rápida, sin comparación. El inconveniente de todo esto es que no hay ningún tipo de protección **técnica** contra la interceptación/grabación y que cualquier persona que tenga el equipo adecuado puede interceptar las comunicaciones con la condición de que pueda acceder al medio de transmisión de estas comunicaciones. La interceptación, si se realiza profesionalmente, no deja ningún o prácticamente ningún rastro. En este contexto, la interceptación ha adquirido una nueva dimensión. El sector bancario fue el primero que recurrió de modo sistemático a la codificación para proteger las comunicaciones a que dio lugar la automatización de las transacciones monetarias. Como consecuencia de la internacionalización cada vez mayor de la economía, este sector también ha recurrido, al menos parcialmente, a la codificación para proteger las comunicaciones. La introducción a gran escala de comunicaciones completamente desprotegidas en Internet incrementó la necesidad que tienen las personas de proteger sus comunicaciones contra las posibles interceptaciones.

En el marco del presente informe se plantea la cuestión de saber si existen métodos de codificación de las comunicaciones que sean económicos, legales, suficientemente seguros y de utilización sencilla que garanticen la protección contra las interceptaciones.

11.1.2. Funcionamiento de la codificación

[159] Hay pruebas en este sentido que se remontan a la Antigüedad como por ejemplo, la utilización del método de codificación con cilindros utilizado por los espartanos en el siglo V.

El principio de la codificación consiste en codificar un texto claro en un texto secreto de modo que no tenga ningún sentido o que tenga un sentido diferente. No obstante, las personas que conocen el sistema pueden devolverlo a su versión original. La codificación convierte una secuencia de letras con sentido en una serie de letras sin sentido que nadie entiende excepto los que conocen la clave.

Esto se hace aplicando un método concreto (algoritmo de la codificación) que se basa en la sustitución (transposición) y/o el intercambio de letras (sustitución). En la actualidad, **el método de la codificación** (algoritmo) no se mantiene en secreto sino todo lo contrario: recientemente se publicó una licitación a nivel mundial relativa a una nueva norma mundial de codificación aplicable a la economía, así como en relación con la adopción de un algoritmo concreto de codificación en forma de soporte informático físico (*hardware*) para aparatos (por ejemplo, un fax criptográfico).

El **verdadero secreto** es la llamada **clave**. La mejor manera de explicar la situación es recurriendo a un ejemplo de un ámbito próximo: por regla general, el funcionamiento de las cerraduras de las puertas es de todos conocido, sobre todo porque están patentadas. Las distintas puertas están protegidas porque para un tipo determinado de cerraduras pueden existir numerosos tipos de llaves distintas. La codificación de la información funciona igual: un **método conocido** de codificación (algoritmo) permite mantener el secreto de **un número importante** de comunicaciones mediante distintas claves **que las personas que las utilizan mantienen en secreto**.

Para explicar los conceptos recogidos anteriormente recurriremos al ejemplo de la llamada "codificación de César". César, el general romano, codificaba los mensajes modificando cada letra por la que le seguía en tercer lugar en el alfabeto, es decir, "A" se convertía en "D", "B" en "E", etc. Así, la palabra **ECHELON** se convertía en **HFKHORQ**. En este caso, el **algoritmo de la codificación** consistía en **la sustitución de letras** dentro del alfabeto, y la **clave** concreta era su sustitución por **la letra que le seguía en tercer lugar en el alfabeto**. Tanto la codificación como la decodificación se realizaban del siguiente modo: la modificación de las letras por las que les seguían en tercer lugar. Se trataba de un sistema simétrico. En la actualidad, la protección que brindaría este sistema no superaría el segundo.

Un buen método de codificación puede ser perfectamente conocido públicamente y, sin embargo, puede considerarse seguro. Para ello es necesario, no obstante, que la cantidad de claves posible sea tan elevada que sea imposible intentarlas todas en un plazo razonable, incluso si se utiliza un ordenador (el llamado ***"ataque con la fuerza bruta" o "brute force attack"***). Por otra parte, la existencia de un número elevado de claves no es una garantía de una seguridad criptográfica si el método de codificación resulta en un texto codificado que incluye claves para su descodificación (por ejemplo, la frecuencia de determinadas letras).[160] Teniendo en cuenta estos dos aspectos, la codificación de César no es segura. Como consecuencia de la distinta frecuencia con que se utilizan las letras en una lengua, su simple sustitución permite encontrar fácilmente la clave teniendo en cuanta que sólo hay 25 combinaciones posibles, es decir, 25 claves, ya que el alfabeto cuenta únicamente con 26 letras. En este caso, el enemigo puede encontrar la clave y descifrar el texto muy rápidamente.

[160] Véase LEIBERICH: *Vom diplomatischen Code zur Falltürfunktion – Hundert Jahre Kryptographie in Deutschland*, Spektrum der Wissenschaft, junio de 1999, p 26 y siguientes.

A continuación, trataremos la cuestión relativa a las características que debe presentar un sistema seguro.

11.2. La seguridad de los sistemas de codificación

11.2.1. Consideraciones de tipo general con respecto al concepto de seguridad de la codificación

Al pedir que un sistema de codificación sea "seguro" se pueden estar pidiendo dos cosas diferentes: por una parte, se puede estar pidiendo que sea totalmente seguro, es decir que no se pueda descifrar el mensaje si no se conoce la clave, y que esta imposibilidad se demuestre matemáticamente. Por otra parte, también podría ser suficiente con que la clave no pueda conocerse teniendo en cuenta la tecnología existente en la actualidad y que, de este modo, presente garantías de seguridad durante un tiempo superior al período "crítico" en el que debe mantenerse el secreto del mensaje.

11.2.2. Seguridad absoluta: *one-time pad*

El único sistema totalmente seguro en la actualidad es el "one-time pad", que se desarrolló a finales de la Primera Guerra Mundial,[161] y que posteriormente se utilizó también en la línea roja de fax entre Moscú y Washington. El sistema se basa en una clave formada por una secuencia totalmente aleatoria de letras no repetitiva. El remitente y el receptor codifican los mensajes con esta secuencia de letras y destruyen la clave después de haberla utilizado por primera vez. Como la clave no tiene ningún orden interno, ningún criptoanalísta puede acceder a la clave, lo que incluso puede demostrar en términos matemáticos.[162]

La desventaja que presenta este sistema es que no es fácil crear grandes cantidades de claves aleatorias de estas características[163] y que la distribución de las claves de modo seguro resulta difícil y poco práctica. Por ello, este sistema no se utiliza en las transacciones comerciales normales.

11.2.3. Seguridad relativa teniendo en cuenta la tecnología existente

11.2.3.1. La utilización de máquinas de codificación y descodificación

Ya antes del haberse inventado el *one-time pad* se habían desarrollado sistemas de codificación que generaban un número elevado de claves y que creaban textos codificados que presentaban la menor cantidad posible de regularidades en el texto, es decir, de elementos que permitían analizar el sistema de codificación. Para que estos sistemas estuviesen listos rápidamente para su utilización se desarrollaron máquinas de codificación y de descodificación. La más espectacular del género fue ENIGMA,[164] utilizada por Alemania

[161] Introducido por el Comandante Joseph Mauborgne, jefe del Servicio de investigación criptográfica del ejército de los EE.UU. Véase SINGH, *Geheime Botschaften*, 1999, p. 151.
[162] Véase SINGH, *Geheime Botschaften*, 1999, p.151 y siguientes.
[163] Véase WOBST, *Abenteur Kryptologie*[2], 1998, p. 60.
[164] ENIGMA: sistema desarrollado por Arthur Scherbius, patentado en 1928. En cierto modo parecía una máquina de escribir, ya que tenía un teclado con el que se escribía el texto original. Mediante un tablero de

durante la Segunda Guerra Mundial. Los numerosos especialistas en codificación que trabajaban en Bletchley Park en Inglaterra fueron capaces de descubrir el código de ENIGMA con la ayuda de máquinas especiales, las llamadas "bombas". Tanto ENIGMA como las "bombas" eran aparatos mecánicos.

11.2.3.2. Utilización de los ordenadores en la criptografía

La invención de los ordenadores supuso una revolución para la criptografía, ya que sus posibilidades permiten la utilización de sistemas cada vez más complejos. Si bien los ordenadores no modificaron los principios básicos de la codificación, no obstante, supusieron cambios. En primer lugar, el grado de complejidad posible de los sistemas de codificación se multiplicó, ya que ya no estaban sujetos a las limitaciones que impone lo posible desde el punto de vista mecánico. En segundo lugar, la velocidad del proceso de codificación aumentó considerablemente.

Los ordenadores procesan la información digitalmente mediante números binarios. Esto quiere decir que la información se traduce en una serie de dos señales: "0" y "1". En términos físicos, "1" equivale a una corriente eléctrica o a una magnetización ("luz encendida"), y "0", a la falta de corriente o de magnetización ("luz apagada"). En este contexto, se ha impuesto la norma ASCII,[165] en la que cada letra está representada por una combinación de siete cifras formada por "0 "y "1".[166] Por lo tanto, los textos se presentan como secuencias de "0" y "1", es decir, en vez de letras se codifican números.

Esta situación permite la utilización de modos de transposición y de sustitución. Por ejemplo, la sustitución puede realizarse mediante la suma de una clave en forma de una serie de números. Según las reglas de las matemáticas binarias, la suma de dos cifras iguales es "0" (es decir, 0+0=0 y 1+1=0) y la de dos cifras distintas es igual a "1" (0+1=1). La nueva secuencia de cifras codificada resultado de la suma es, por consiguiente, una secuencia binaria, que puede procesarse digitalmente o que puede hacerse legible de nuevo si se sustrae la clave añadida.

Los ordenadores permiten generar textos codificados mediante la utilización de algoritmos de codificación potentes que prácticamente no ofrecen ninguna posibilidad para realizar análisis criptológicos. Las posibilidades de descodificación se reducen a intentar todas las claves posibles. Cuanto mayor sea la clave, mayores son las posibilidades de que fracase este método, incluso aunque se utilicen ordenadores muy potentes durante el tiempo que sea necesario. Por consiguiente, existen métodos que se pueden utilizar que se pueden considerar seguros teniendo en cuenta la tecnología existente en la actualidad.

11.2.4. Normalización y limitación consciente de la seguridad

Como consecuencia de la propagación de los ordenadores en los años 70, la normalización de los sistemas de codificación se convirtió en una necesidad cada vez mayor, ya que ésta era la

---

clavijas y unos rodillos, el texto se codificaba según unas normas concretas y se descodificaba con la misma máquina mediante códigos.

[165] American Standard Code for Information Interchange.

[166] A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, etc.

única forma que tenían las empresas para comunicarse con garantías de seguridad con sus interlocutores comerciales sin incurrir en costes desproporcionados. Los primeros pasos en este sentido se dieron en los EE.UU.

Los sistemas potentes de codificación también pueden utilizarse para fines ilegales o por un enemigo militar potencial. Asimismo, pueden dificultar o hacer imposible el espionaje electrónico. Por ello, la NSA insistió en que a las empresas se les ofreciese un sistema de codificación con un nivel de seguridad suficiente que le permitiese conservar a si misma la posibilidad de descodificar debido a sus posibilidades técnicas concretas. En este contexto, la longitud de los códigos se limitó a 56 bits, lo que reduce el número de posibles códigos a 100 000 000 000 000 000.[167] El 23 de noviembre de 1976 se adoptó oficialmente la llamada "cifra de Lucifer", de Horst Feistel, en su **versión de 56 bits**, con el nombre de Data Encryption Standard (DES), que durante un cuarto de siglo fue la norma oficial de codificación de los Estados Unidos.[168]En Europa y en Japón también se adoptó esta norma, en particular en el sector bancario. A pesar de las afirmaciones aparecidas en distintos medios, el algoritmo DES no se ha descubierto, si bien en la actualidad hay hardware con la potencia suficiente como para intentar todas las claves ("brute force attack"). Por el contrario el Triple-DES, que tiene una clave de 112 bits, sigue considerándose seguro. El sucesor de DES, el AES (Advanced Encryption Standard) es un método europeo[169] desarrollado bajo el nombre de Rijndael en Lovaina, Bélgica. **Se trata de un sistema rápido que se considera seguro, ya que no se basa en la limitación del tamaño de las claves**, lo que se debe a una modificación en la política de los EE.UU. en materia de criptología (véase el apartado 11.1.4 recogido anteriormente).

Para las empresas, la normalización ha significado una clara simplificación de la codificación. No obstante, sigue planteándose el problema de la distribución de las claves.

11.3. El problema de la distribución/ transmisión segura de las claves

11.3.1. Codificación asimétrica: el procedimiento de la clave pública

En la medida en que un sistema funcione con una clave que sirve tanto para codificar como para descodificar (codificación simétrica), resulta muy difícil poder utilizarla con un **número elevado** de interlocutores. La clave debe comunicarse a cada nuevo interlocutor **con anterioridad** de tal modo que no pueda conocerla ningún tercero. Desde el punto de vista práctico, esto no es fácil para el sector económico y, para los particulares, sólo es posible en algunos casos concretos.

La codificación asimétrica es una solución a este problema: para la codificación y la descodificación se utilizan claves diferentes. El mensaje se codifica con una clave (la llamada **clave pública)** que puede ser de dominio público. Este sistema funciona únicamente como una vía de dirección única, es decir, en una sola dirección: con la clave pública ya no se puede

[167] Esta cifra, en términos binarios, está formada por 56 "0" y "1". Véase SINGH, *Geheime Botschaften,* 1999, o3.
[168] Véase SINGH, *Geheime Botschaften,* 1999, p. 302 y siguientes.
[169] Creado por dos criptógrafos belgas de la Universidad Católica de Lovaina, Joan Daemen y Vincent Rijmen.

descodificar el texto. Por ello, las personas que deseen recibir un mensaje codificado también pueden enviar a su interlocutor su clave pública por una vía no segura para codificar el mensaje. Para descodificarlo se utiliza otra clave, la **clave privada**, que se mantiene en secreto y que no se envía.[170] Para entender este sistema, lo más sencillo es compararlo con un candado: cualquiera puede cerrarlo y, de este modo, cerrar con seguridad un baúl. Sin embargo, sólo puede abrirlo quien tiene la llave correcta.[171] Las claves pública y privada están interrelacionadas, pero la clave privada no puede descifrarse a partir de la clave pública.

Ron Rivest, Adi Shamir y Leonard Adleman descubrieron un sistema de codificación asimétrica que ha recibido su nombre (el sistema RSA). El resultado de la multiplicación de dos números primarios muy elevados se convierte en uno de los elementos de la clave pública sobre la base de una función unívoca (la llamada "función escotilla"). Así es como se codifica el texto. La descodificación sólo puede llevarla a cabo quien conoce los dos números primarios utilizados. No obstante, no hay ningún procedimiento matemático que permita calcular, a partir de la multiplicación, los números primarios utilizados. Hasta la fecha, la única forma de hacerlo es mediante pruebas sistemáticas. Por ello, teniendo en cuenta el estado de los conocimientos actuales, este sistema es seguro siempre que se escojan números primarios suficientemente elevados. El único riesgo que se puede correr es que en un momento dado un matemático brillante pueda encontrar una vía más rápida para descomponer los factores. Hasta la fecha, no obstante, no se ha conseguido, a pesar de los esfuerzos desplegados en este sentido.[172] Son muchos los que consideran que el problema es irresoluble si bien todavía no se han presentado pruebas concretas en este sentido.[173]

Si se compara con el procedimiento simétrico (por ejemplo, DES), la codificación basada en una clave pública impone al ordenador una capacidad de procesamiento mucho mayor o la utilización de ordenadores rápidos de gran tamaño.

11.3.2. Codificación basada en un clave pública para los particulares

Para generalizar el acceso al sistema basado en la clave pública, Phil Zimmerman tuvo la idea de asociar este sistema, que implica numerosos cálculos, a un procedimiento simétrico más rápido. El mensaje se codificaba mediante un procedimiento simétrico (el procedimiento IDEA desarrollado en Zürich) y, por su parte, la clave de la codificación simétrica se transmitía simultáneamente de conformidad con el sistema de la clave pública. Zimmermann desarrolló un programa fácil de utilizar llamado Pretty Good Privacy, que creaba las claves necesarias al golpear una tecla (o el ratón) y efectuaba la codificación. El programa se puso en Internet, de donde puede bajarlo cualquiera. En último término, la empresa norteamericana NAI compró el programa PGP, si bien sigue estando gratuitamente a disposición de los particulares.[174] El código fuente de las anteriores versiones se publicó, por lo que se puede partir de la base de que no se añadieron "puertas falsas". Lamentablemente, los textos originales de la versión más reciente, la PGP 7, que se caracteriza por tener una interfaz gráfica de muy fácil utilización, no se han publicado.

---

[170] La idea de la codificación asimétrica que utiliza el sistema de la clave publica es de Whitfield Diffie y Martin Hellmann.
[171] SINGH, *Geheime Botschaften*, 1999, p. 327.
[172] Véase BUCHMANN, *Faktorisierung großer Zahlen,* Spektrum der Wissenschaft 2 1999, p. 6.
[173] Véase SINGH, *Geheime Botschaften*, 1999, p. 335 y siguientes.
[174] Se encuentra información sobre este software en www.pgpi.com.

En realidad, existe otra aplicación de la norma abierta PGP: elGnuPG, que presenta los mismos sistemas de codificación que el PGP y que también es compatible con éste. No obstante, se trata de software gratuito, su código es conocido y cualquier persona puede utilizarlo y transmitirlo. El Ministerio Federal de Economía y Tecnología de Alemania ha impulsado la introducción de GnuPG en Windows y el desarrollo de una interfaz gráfica. Hay que lamentar que esto todavía no se haya llevado totalmente a la práctica. Según informaciones recibidas por el ponente, se está trabajando en ello.

Hay que señalar, asimismo, que hay una serie de normas que compiten con OpenPGP, como S/MIME, que está apoyado por distintos programas de correo electrónico. El ponente no dispone de ningún tipo de información en relación con su aplicación gratuita.

11.3.3. Procedimientos futuros

En el futuro, la criptografía cuántica podría abrir vías totalmente nuevas en relación con la transmisión segura de claves, ya que garantiza la detección de una interceptación durante la transmisión de una clave. Con respecto a la transmisión de fotones polarizados, la polarización no puede detectarse sin llevar a cabo una modificación. De ese modo, las interceptaciones pueden detectarse fácilmente. En ese caso sólo se utilizaría una clave que no pudiese interceptarse. En los ensayos se han llevado a cabo con éxito transmisiones a lo largo de 40 Km de cable de fibra óptica y en 500 m. en el aire.[175]

11.4. La seguridad de los productos codificados

En el debate sobre la seguridad que realmente ofrece la codificación siempre se ha criticado que los productos de los EE.UU. presentan "puertas falsas" (*"backdoor"*). Excel, por ejemplo, fue objeto de distintos titulares en los medios de comunicación al afirmarse que en la versión europea la mitad de la clave aparece claramente en la cabecera del documento. La prensa centró su atención en Microsoft porque un *"hacker"* encontró escondida en el programa una clave de la NSA, lo que, obviamente, Microsoft desmintió enérgicamente. Como Microsoft no reveló su código original, cualquier afirmación al respecto no es más que pura especulación. En el caso de las versiones anteriores de PGP y de GnuPG, se puede excluir con toda seguridad la existencia de una "backdoor" de estas características, ya que ha dado a conocer su código original.

11.5. Codificación en conflicto con intereses estatales

11.5.1. Intentos de limitación de la codificación

Son muchos los Estados que prohiben la utilización de software destinado a la codificación o de aparatos de codificación y las únicas excepciones que autorizan están sometidas a permisos. No se trata únicamente de Estados dictatoriales como, por ejemplo, China, Irán o Irak: también algunos Estados democráticos han limitado por ley la utilización o la venta de programas o instrumentos de codificación. Si bien las comunicaciones deben estar protegidas de la posibilidad de que puedan leerlas personas no autorizadas, el Estado debe reservarse la

[175] Con respecto a la criptografía cuántica, véase WOBST, *Abenteuer Kryptographie*[2] *1998, p.234.*

posibilidad de interceptarlas legalmente, como siempre ha ocurrido. La pérdida por parte de las autoridades de la superioridad técnica debe compensarse por medio de prohibiciones jurídicas. En este sentido, Francia ha prohibido totalmente hasta hace poco la utilización de la criptografía, y la ha supeditado a autorizaciones especiales caso por caso. En Alemania también se registró hace unos años un debate sobre las limitaciones de la codificación y la obligación de presentar una clave. Por el contrario, los EE.UU. limitaron en el pasado las dimensiones de las claves.

11.5.2. La importancia de la codificación segura para el comercio electrónico

Hoy por hoy, estos intentos deberían darse por fracasadas definitivamente. Frente al interés del Estado de acceder a los sistemas de descodificación y, por consiguiente, a textos claros, se oponen no sólo el derecho a la intimidad sino también intereses económicos importantes. El comercio electrónico y las transacciones bancarias electrónicas dependen de que las comunicaciones por Internet sean seguras. Si no se pueden garantizar unas comunicaciones seguras, estas técnicas están condenadas al fracaso, ya que los clientes perderían la confianza que tienen. Esta relación explica el cambio registrado en las políticas de los EE.UU. o de Francia en relación con la criptología.

Cabe señalar que hay dos razones por las que para el comercio electrónico son necesarios sistemas de codificación seguros: no sólo para codificar mensajes, sino, también, para poder establecer sin ningún género de dudas la identidad de su interlocutor comercial. La firma electrónica puede funcionar si se invierte el procedimiento de la clave pública: la clave privada se utiliza para la codificación y la pública para la descodificación. Esta forma de codificación confirma la autenticidad de la firma. Mediante la utilización de la clave pública cualquier persona puede convencer a otra de su autenticidad, si bien no puede imitar la firma. La PGP también ofrece esta función, que es fácil de utilizar.

11.5.3. Problemas para los viajantes de comercio

En algunos Estados, los viajantes de comercio no pueden utilizar en sus ordenadores portátiles programas de codificación, lo que impide todo tipo de protección de las comunicaciones con sus propias empresas y la seguridad de los datos que llevan consigo frente a posibles ataques.

11.6. Cuestiones prácticas relacionadas con la codificación

Para contestar a la pregunta de quién puede tener acceso a la codificación y en qué circunstancias parece oportuno hacer una diferenciación entre particulares y empresas. En lo que respecta a los particulares, hay que señalar claramente que no se pueden codificar los fax ni las conversaciones telefónicas mediante un teléfono criptográfico o un apartado de fax codificado, no sólo porque la compra de estos aparatos supone un desembolso relativamente importante sino, también, porque su utilización presupone que el interlocutor también dispone de este equipo, lo que no es muy frecuente.

Por el contrario, cualquiera debería tener la posibilidad de proteger el correo electrónico codificándolo. A la afirmación que se hace con frecuencia en el sentido de que las personas no tienen secretos y que, por lo tanto, no tienen necesidad de codificar sus mensajes, cabe

responder que, por regla general, las informaciones escritas no se transmiten en postales. Un correo electrónico sin codificar se puede comparar a una carta enviada sin sobre. La codificación del correo electrónicos es segura y relativamente sencilla. En Internet se encuentran sistemas de fácil utilización, como, por ejemplo, PGP/GnuPG, que están a disposición de los particulares de modo gratuito. No obstante, aún no están suficientemente expandidos. Sería de desear que las instancias públicas diesen ejemplo y recurriesen a la codificación para desmitificarla.

En lo que se refiere a las empresas, habría que adoptar medidas para que las informaciones importantes sólo se transmitan por vías de comunicación seguras, lo que parece una obviedad, sobre todo en el caso de las grandes empresas, pero, también en particular, en el de las PYME, ya que frecuentemente transmiten por correo electrónico informaciones internas sin codificar porque no conocen adecuadamente este problema. En este contexto, cabe esperar que las organizaciones empresariales y las cámaras de comercio multipliquen sus esfuerzos para aumentar el grado de información al respecto. No cabe duda de que la codificación del correo electrónico no es más que un aspecto relacionado con la seguridad entre otros muchos y que no tiene sentido si la información ya se ha transmitido a terceros antes de la codificación. Esto quiere decir que hay que proteger todo el entorno de trabajo para garantizar la seguridad de los locales que se utilizan, así como que hay que establecer controles en relación con el acceso físico a las oficinas y a los ordenadores. Además, hay que impedir el acceso no autorizado a la información a través de la red mediante la creación de fire-walls (barreras de protección). En este contexto, la interconexión de la red interna (Intranet) y de Internet presenta riesgos concretos. Si la seguridad se toma en serio, sólo deben utilizarse sistemas cuyo código sea público y se haya comprobado, ya que éste es el único modo de poder decir con seguridad lo que ocurre con los datos. Por consiguiente, las empresas tienen mucho que hacer en relación con la seguridad. En el mercado son ya muchas las empresas que ofrecen a precios razonables sus servicios en materia de asesoramiento y en cuestiones relacionadas con la seguridad. La oferta de este tipo de servicios aumenta en la medida en que se incrementa la demanda. Asimismo, cabe esperar que las asociaciones empresariales y las cámaras de comercio aborden estos problemas, en particular para sensibilizar a las pequeñas empresas con respecto a la problemática en materia de seguridad y para ayudarlas a definir y a aplicar un marco mundial de protección.

12. Las relaciones exteriores de la UE y la recogida de información por los servicios de inteligencia

12.1. Introducción

La aprobación del Tratado de Maastricht en 1991 supuso el establecimiento de las bases de la Política Exterior y de Seguridad Común (PESC) como nuevo instrumento político de la Unión Europea. Seis años más tarde, el Tratado de Amsterdam consolidó la PESC y brindó la posibilidad de adoptar iniciativas comunes en el ámbito de la defensa en la Unión Europea, si bien mantenía las alianzas existentes. Basándose en el Tratado de Amsterdam y teniendo en cuenta las experiencias recogidas en Kosovo, el Consejo Europeo de Helsinki de diciembre de 1999 lanzó la Iniciativa europea se seguridad y defensa, cuyo objetivo es el establecimiento antes de que finalice el segundo semestre de 2001 de una fuerza multinacional compuesta por unas 50-60.000 fuerzas armadas. Esta fuerza internacional desembocará inevitablemente en el establecimiento de una entidad autónoma en el ámbito de la información. Para ello, la simple integración de las estructuras existentes en la UEO no será suficiente. Asimismo, será inevitable reforzar la cooperación entre los servicios de inteligencia de los Estados miembros más allá de las formas de cooperación existentes en la actualidad.

No obstante, el desarrollo de la PESC no es el único elemento que conllevará una mayor integración de los servicios de inteligencia de la Unión: la integración económica dentro la Unión también hará necesaria una cooperación más intensa en el ámbito de la recogida de información por estos servicios. Una política económica europea común presupone una percepción común de la realidad económica existente fuera de la Unión Europea. El mantenimiento de una posición común en las negociaciones comerciales en el marco de la OMC o con respecto a terceros países implica la defensa común de la posición mantenida en las negociaciones. Unas empresas europeas fuertes necesitan una protección común frente al espionaje económico que se registra desde fuera de las fronteras de la Unión Europea.

Para terminar, hay que subrayar que la profundización del segundo pilar de la Unión y de las actividades de la Unión en el ámbito de los asuntos de interior y justicia debe implicar, también, una mayor cooperación entre los servicios de inteligencia. En concreto, la lucha conjunta contra el terrorismo, el tráfico ilícito de armas, el tráfico de personas y el blanqueo de dinero no pueden llevarse a cabo si los servicios de inteligencia no cooperan intensamente entre sí.

12.2. Posibilidad de cooperación en la UE

12.2.1. Cooperación existente en la actualidad

Si bien hay una larga tradición en los distintos servicios de inteligencia de confiar únicamente en la información que recaban ellos mismos e, incluso, de desconfiar los unos de los otros, la cooperación entre estos servicios está aumentando gradualmente y se registran contactos frecuentes en el marco de la OTAN, de la UEO y de la Unión Europea. Si bien los servicios de inteligencia de la OTAN siguen dependiendo en gran medida de las contribuciones mucha más sofisticadas de los Estados Unidos, la creación del Centro de seguimiento de satélites de

Torrejón (España) y de una sección de información en el cuartel general de la UEO han contribuido a que las acciones de Europa en este ámbito tengan mayor autonomía.

12.2.2. Ventajas de una política común europea en el ámbito de la información

Además de los hechos que se están registrando en la actualidad, hay que subrayar que el establecimiento de una política común europea en el ámbito de la información tendría sus ventajas, que se recogen a continuación:

12.2.2.1. Ventajas de orden práctico

En primer lugar, el volumen del material clasificado y no clasificado existente es demasiado elevado para poder ser recopilado, analizado y evaluado por una única agencia o mediante acuerdos bilaterales en Europa Occidental. Las actividades de los servicios de inteligencia van desde la defensa hasta las políticas económicas nacionales e internacionales de terceros países, pasando por el apoyo a la lucha contra la delincuencia organizada y el tráfico de estupefacientes. Incluso en el caso de que esta cooperación sólo se registrase al nivel más básico, por ejemplo en lo que se refiere a la recogida de información de acceso generalizado (OSINT), los resultados de este tipo de cooperación tendrían una gran importancia para las políticas de la Unión Europea.

12.2.2.2. Ventajas de carácter financiero

En los últimos años, los presupuestos destinados a la recogida de datos por los servicios de inteligencia se han recortado y, en algunos casos, siguen recortándose. Paralelamente, la demanda de información ha ido en aumento. Estos presupuestos reducidos no sólo hacen que esta cooperación sea posible sino, también, que a largo plazo resulte ventajosa en términos financieros. En concreto, en lo que se refiere al establecimiento y el mantenimiento de las infraestructuras técnicas, las operaciones conjuntas resultan interesantes cuando hay escasez de recursos, así como cuando se evalúa la información recopilada. La profundización de la cooperación aumentará el grado de eficacia de la recogida de información por los servicios de inteligencia.

12.2.2.3. Ventajas políticas

En principio, la información recogida se utiliza para que los gobiernos puedan adoptar decisiones en mejores condiciones y con más elementos de base. La profundización del grado de integración política y económica de la Unión Europea implica que la información estará accesible a nivel europeo, así como que se basará en más de una fuente.

12.2.3. Conclusiones

Estas ventajas objetivas ilustran la importancia cada vez mayor que tiene la cooperación en la Unión Europea. En el pasado, los Estados-Nación garantizaban, cada uno para si, la seguridad exterior, el orden interno, la prosperidad nacional y la identidad cultural. Hoy por hoy, la Unión Europea está en vías de desempeñar en muchos ámbitos un papel que es, cuanto

menos, complementario al de los Estados-Nación. Es difícil pensar que los servicios de inteligencia se conviertan en el último y único ámbito al que no afecte la integración europea.

12.3. La cooperación más allá de la Unión Europea

Desde la Segunda Guerra Mundial, la cooperación en el ámbito de la recogida de información no se ha llevado a cabo básicamente a nivel europeo sino, por el contrario, a nivel transatlántico. Ya se ha dicho anteriormente que el Reino Unido y los Estados Unidos establecieron una relaciones muy estrechas en relación con la recogida de información. No obstante, en lo que se refiere a la recogida de información en materia de defensa en el marco de la OTAN y fuera de ella, los Estados Unidos han sido y siguen siendo la potencia dominante. Por consiguiente, la pregunta más importante es saber si el refuerzo de la cooperación europea en el ámbito de la recogida de información repercutirá negativamente sobre las relaciones con los Estados Unidos o si generará un fortalecimiento de estas relaciones. ¿Cómo se van a desarrollar las relaciones entre la UE y los EE.UU. durante el mandato de Bush? Y, en particular, ¿cómo se van a desarrollar en este ámbito las relaciones especiales que mantienen los EE.UU. y el Reino Unido? Algunos observadores consideran que la relación especial que mantienen el RU y los EE.UU. y la profundización de la PESC no tiene por que suponer contradicción alguna. Otros afirman que el tema de la recogida de información puede ser el que haga decidirse al Reino Unido por un destino europeo o transatlántico. Posiblemente, las estrechas relaciones que mantiene el Reino Unido con los EE.UU. (y con los demás países que participan en el Acuerdo UKUSA) plantee problemas a los demás Estados miembros de la UE en lo que se refiere a compartir información entre si, ya que el Reino Unido podría tener menos interés en compartir información con sus socios europeos y sus socios de la UE podrían confiar menos en el Reino Unido. Además, si los EE.UU. llegan a la conclusión de que el Reino Unido ha establecido vínculos especiales con sus interlocutores de la UE y que forma parte de un acuerdo especial europeo podrían hacerse reacios a seguir compartiendo su información con el Reino Unido. Por consiguiente, la profundización de la cooperación en la UE en el ámbito de la información puede convertirse en una prueba importante para las ambiciones europeas del Reino Unido y para la capacidad de integración de la propia UE.

No obstante, en el contexto actual, es muy improbable que incluso avances muy rápidos en la cooperación entre los socios europeos puedan superar, a corto o medio plazo, la ventaja que tienen los EE.UU. desde el punto de vista tecnológico. La Unión Europea no estará en condiciones de crear una red sofisticada de satélites SIGNIT, de satélites de obtención de imágenes y de bases terrestres. A corto plazo, la Unión Europea no estará en condiciones de desarrollar la red altamente sofisticada de ordenadores necesaria para seleccionar y evaluar las informaciones recogidas. La Unión Europea no estará dispuesta a movilizar los recursos presupuestarios necesarios para convertirse en una verdadera alternativa a los esfuerzos que realizan los EE.UU. en este ámbito. Por consiguiente, y desde una perspectiva tecnológica y financiera, la Unión Europea estará interesada en mantener una relación estrecha con los EE.UU. en lo que se refiere a la recogida de información. Además, desde el punto de vista político, será muy importante mantener, y en aquellos casos en que sea posible, reforzar la relación con los Estados Unidos en particular en lo que se refiere a la lucha conjunta contra la delincuencia organizada, el terrorismo, el tráfico de estupefacientes y de armas, y el blanqueo de dinero. Son necesarias acciones comunes para apoyar esfuerzos comunes. Acciones

comunes en materia de mantenimiento de la paz como las registradas en la antigua Yugoslavia suponen una mayor contribución europea en todas las esferas de actuación.

Por otra parte, el aumento de la concienciación europea al respecto debe ir acompañado de una mayor responsabilidad europea. La Unión Europea debe convertirse en un socio a partes iguales, no sólo en el ámbito económico sino también en el de la defensa y, por consiguiente, en el de la recogida de información. Por lo tanto, la existencia de una capacidad europea con mayor autonomía en el ámbito de la información no debe considerarse un debilitamiento de las relaciones transatlánticas sino que, por el contrario, debe contribuir a que la Unión Europea se convierta en un socio situado en el mismo plano y más competente. Además, la Unión Europea debe realizar un esfuerzo autónomo para proteger su economía y su industria contra las amenazas ilegales e indeseables como el espionaje económico, la delincuencia cibernética y los ataques terroristas. Por otra parte, es necesario un consenso transatlántico en el ámbito del espionaje industrial. La Unión Europea y los Estados Unidos deberían legar a un acuerdo sobre una serie de normas en lo que se refiere a lo que se permite y lo que no se permite en esté ámbito. Para reforzar la cooperación transatlántica en relación con este aspecto debería adoptarse una iniciativa conjunta a nivel de la OMC para utilizar los mecanismos de esta organización con vistas a lograr un desarrollo económico justo en todo el mundo.

12.4. Consideraciones finales

El punto más importante, es decir, la protección de la esfera privada de los ciudadanos europeos, sigue teniendo interés. No obstante, el desarrollo de una entidad común de la Unión Europea debe seguir considerándose necesario e inevitable. Debe mantenerse, y muy posiblemente, reforzarse la cooperación con los terceros países y, en particular, con los Estados Unidos, lo que no quiere decir que las actividades europeas en relación con la SIGINIT deban integrarse automáticamente en un sistema ECHELON independiente de la Unión Europea o que la Unión Europea deba convertirse en un miembro activo del Acuerdo UKUSA. Sin embargo, hay que examinar en profundidad la posibilidad de establecer una verdadera entidad europea en el ámbito de la recogida de información. La existencia de una entidad europea integrada en el ámbito de la información implica, además, un sistema europeo de control político sobre las actividades de estos organismos. Deberán adoptarse decisiones en relación con el modo de analizar la información y habrá que adoptar las decisiones políticas que se deriven del análisis. La falta de un sistema de control político y, por consiguiente, de conciencia y responsabilidad política en relación con el procedimiento de recogida de información sería perjudicial para el proceso de integración europea.

13. Consideraciones finales y recomendaciones

13.1. Consideraciones preliminares

En este capítulo se recogen experiencias y posibles conclusiones. No debe considerarse definitivo. Por el contrario, el ponente desea, más bien, sentar las bases del debate político que se debe llevar ahora a cabo en la comisión. En el futuro habrá que volver a modificar el texto para poder incorporar distintos aspectos de este debate.

13.2. Conclusiones

Con respecto a la existencia de un sistema mundial de interceptación de las comunicaciones privadas y económicas (sistema de interceptación ECHELON)

No hay ninguna razón para seguir dudando de la existencia de un sistema de interceptación de las comunicaciones a nivel mundial en el que participan los EE.UU., el Reino Unido, Canadá, Australia y Nueva Zelanda en el marco del Acuerdo UKUSA. Teniendo en cuenta las informaciones existentes es probable que su nombre sea realmente "ECHELON"; sin embargo, éste no es un aspecto de importancia primordial. Lo importante es que sirve para interceptar comunicaciones privadas y de carácter económico, pero no militares.
Los análisis han demostrado que este sistema no puede tener, ni por asomo, las dimensiones que en parte han supuesto los medios de comunicación.

Con respecto a los límites del sistema de interceptación

El sistema de interceptación se basa en la interceptación a escala mundial de las comunicaciones por satélite. No obstante, en las regiones con una densidad elevada de comunicaciones, el porcentaje de las comunicaciones realizadas por satélite es muy limitado, lo que implica que la mayor parte no pueden interceptarse desde estaciones terrestres sino mediante la interceptación de cables o por radio. No obstante, las investigaciones han demostrado que los Estados participantes en el sistema ECHELON sólo tienen acceso a un porcentaje muy escaso de las comunicaciones por cable y radio y que sólo pueden examinar una parte limitada de las comunicaciones debido a la escasez de personal.

Con respecto a la existencia de otros sistemas de interceptación

Teniendo en cuenta que la interceptación de las comunicaciones en un medio de espionaje tradicional de los servicios de inteligencia, otros Estados también podrían utilizar un sistema similar si dispusiesen de los recursos financieros y de las condiciones geográficas adecuadas. Gracias a los territorios de ultramar de los que dispone, Francia sería, por lo menos en lo que se refiere a las condiciones geográficas, el único Estado miembro de la UE que podría establecer un sistema de interceptación mundial. Disponemos de indicios que permiten afirmar que Rusia también podría explotar un sistema de estas características.

Con respecto a su compatibilidad con el Derecho de la UE

En relación con la compatibilidad de un sistema de las características del sistema ECHELON con el Derecho de la UE hay que hacer dos precisiones: si el sistema se utilizase exclusivamente para fines de información, no habría ningún tipo de contradicción con el Derecho de la UE en la medida en que el Tratado CE no aborda las cuestiones relacionadas con las actividades en el ámbito de la seguridad nacional sino que entran dentro del ámbito

del Título V del TUE (PESC), si bien, hoy por hoy, no incluye ningún tipo de disposiciones en la materia, por lo que no plantea ningún problema. Por el contrario, si el sistema se utilizase de manera abusiva para espiar a la competencia, sería incompatible con el principio de lealtad que deben respetar los Estados miembros y con el concepto de un mercado común en el que la competencia es libre. La participación de un Estado miembro en un sistema de estas características sería incompatible con el Derecho comunitario.

En relación con la compatibilidad con el principio fundamental del respeto a la vida privada (artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales)

Toda interceptación de las comunicaciones supone una injerencia grave contra la vida privada de la persona. El artículo 8 del Convenio al que se ha hecho referencia anteriormente, que garantiza el respecto a la vida privada, únicamente permite este tipo de injerencias cuando son necesarias para garantizar la seguridad nacional, en la medida en que estén previstas en el Derecho nacional y sean accesibles a todos. Asimismo, deben definirse las condiciones en las que las autoridades pueden adoptarlas. Estas injerencias deben ser proporcionadas, por lo que debe establecerse un equilibrio entre los intereses en juego, ya que no es suficiente que esta acción sea necesaria o deseable.

Un sistema de información que interceptase todos los mensajes que no tuviese en cuenta el principio de proporcionalidad sería contrario a este Convenio, como también lo sería si las disposiciones en las que se apoyase la interceptación de las comunicaciones no se basasen en un fundamento jurídico, si no fuesen accesibles a todos, o si se formulasen de tal modo que sus consecuencias sobre los particulares fuesen impredecibles. Teniendo en cuenta que las disposiciones en las que se basan las actividades de los servicios de inteligencia de los EE.UU. en el extranjero son secretas en su mayoría, el respeto del principio de proporcionalidad es, cuanto menos, dudoso. Se violarían los principios recogidos en este Convenio relativos al acceso al Derecho y a la previsión de sus repercusiones. Si bien los EE.UU. no son parte contratante de este Convenio, los Estados miembros deben actuar de conformidad con él. Asimismo, no pueden incumplir las obligaciones que de él se derivan aduciendo que permiten operar en su territorio a los servicios de inteligencia de otros Estados que están sometidos a unas disposiciones menos estrictas. De no ser así, el principio de la legalidad, basado en sus dos componentes, el acceso y su previsión, no sería eficaz y se socavaría el espíritu de la jurisprudencia de este Convenio.

Para que las actividades legales de los servicios de inteligencia sean compatibles con los derechos fundamentales es necesaria, además, la existencia de suficientes mecanismos de control para contrarrestar los peligros que conllevan las actividades secretas de determinados segmentos del aparato de la administración. Teniendo en cuenta que el Tribunal Europeo de Derechos Humanos ha subrayado expresamente la importancia que revisten unos sistemas de control eficaces en el ámbito de las actividades de los servicios de inteligencia, resulta preocupante que algunos de los Estados miembros no dispongan de órganos de control parlamentario de los servicios de inteligencia.

En relación con la cuestión relativa al grado de protección de los ciudadanos de la UE con respecto a los servicios de inteligencia

Teniendo en cuenta que la protección de los ciudadanos de la UE depende de la situación jurídica en los distintos Estados miembros, y que esta es muy distinta en los diferentes

Estados, ya que en algunos casos no hay ningún órgano de control parlamentario, es difícil poder hablar de la existencia de un grado de protección adecuado. Para los ciudadanos europeos es muy importante que sus Parlamentos nacionales cuenten con una comisión de control especial con una estructura formal que controle y examine las actividades de los servicios de inteligencia. Incluso en aquellos países que cuentan con órganos de control, la tentación de preocuparse en mayor medida de las actividades de los servicios nacionales de inteligencia que de los extranjeros es grande, ya que, por regla general, a los ciudadanos sólo les afectan los primeros.
En caso de cooperación entre los servicios de inteligencia en el marco de la PESC, las instituciones deben adoptar unas disposiciones de protección suficiente de los ciudadanos europeos.

En relación con el espionaje económico
Uno de los aspectos que se incluyen en el ámbito de competencia de los servicios de inteligencia en el extranjero es interesarse por los datos económicos tales como el desarrollo de los distintos sectores, la evolución de los mercados de materias primas, el respeto de los embargos económicos, el cumplimiento de las disposiciones relativas al suministro de bienes de doble uso, etc. Esta es la razón por la que frecuentemente se vigila a las empresas que realizan sus actividades en estos ámbitos. La situación se hace intolerable cuando los servicios de inteligencia se dejan instrumentalizar para espiar a la competencia y espían a las empresas extranjeras para conseguir ventajas competitivas para las empresas nacionales. Si bien son muchos los que afirman que esta fue la razón por la que se creó en sistema de interceptación mundial, no hay pruebas al respecto. En realidad, las informaciones sensibles relativas a las empresas se encuentran, sobre todo, en las propias empresas, de modo que el espionaje se realiza, básicamente, obteniendo información a través de los colaboradores o de las personas infiltradas o, si no, entrando en las redes informáticas. Los sistemas de interceptación de comunicaciones para el espionaje industrial sólo pueden utilizarse cuando las informaciones sensibles se transmiten al exterior por cable o radio (satélite), lo que se aplica sistemáticamente en los tres casos que figuran a continuación:

- cuando las empresas trabajan en las tres franjas horarias, de modo que los resultados parciales correspondientes a Europa se transmiten a América y, a continuación, a Asia;
- cuando los consorcios internacionales celebren videoconferencias por satélite o cable;
- cuando se negocian in situ contratos importantes (por ejemplo, construcción de plantas industriales, infraestructuras de telecomunicaciones, construcción de sistemas de transporte, etc.) y es necesario hablar con la sede central de la empresa.

Con respecto a la posibilidad de autoprotección
Las empresas deben proteger todo el entorno de trabajo así como todos los medios de comunicación por los que se transmiten informaciones sensibles. En el mercado europeo existen suficientes sistemas de codificación con un grado de seguridad suficiente a precios asequibles. También se debe instar a las personas a que codifiquen urgentemente el correo electrónico, ya que un mensaje sin codificar es como una carta sin sobre. En Internet hay sistemas relativamente fáciles de utilizar que están a disposición de los particulares, algunos de ellos gratuitos.

Con respecto a una colaboración con los servicios de inteligencia en el seno de la UE

La UE ha decidido coordinar la recogida de información por servicios de inteligencia en el marco del desarrollo de una política de seguridad y de defensa propia, así como continuar su colaboración con sus demás socios. La cooperación entre los servicios de inteligencia existentes en la UE resulta deseable toda vez que, por una parte, una política de seguridad común que excluyese los servicios de inteligencia no tendría sentido y, por otra, implicaría numerosas ventajas desde el punto de vista profesional, financiero y político. Además, también sería compatible con la idea de convertirse en socio de los EE.UU. en igualdad de condiciones y podría reagrupar al conjunto de los Estados miembros en un sistema que fuese plenamente compatible con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales. En este caso, debería garantizarse que el Parlamento Europeo pudiese ejercer el control que le corresponde. El Parlamento está estudiando una serie de disposiciones propias relativas al acceso a informaciones y documentos confidenciales y sensibles.

13.3. Recomendaciones

Con respecto a la celebración y la modificación de Tratados internacionales sobre la protección de los ciudadanos y de las empresas

1. Se insta al Secretario General del Consejo de Europa a que presente al Comité de ministros un estudio sobre la oportunidad de adaptar a los métodos de comunicación y a las posibilidades de interceptación existentes en la actualidad las disposiciones del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales que garantizan la protección de la vida privada en un protocolo adicional o conjuntamente con las disposiciones relativas a la protección de los datos en el marco de una revisión de la Convención relativa a la protección de la información con la condición de que esto no se traduzca en una reducción del nivel de protección adoptado por el Tribunal ni en una reducción de la flexibilidad necesaria para la adaptarse a los acontecimientos que se produzcan en el futuro;

2. Se insta a los Estados miembros a que creen una plataforma europea para examinar las disposiciones legales relativas al respeto del secreto de la correspondencia y de las comunicaciones, a que lleguen a un acuerdo sobre un texto común que garantice a todos los ciudadanos europeos que residan en el territorio de los Estados miembros la protección de la vida privada tal y como se define en el artículo 7 de la Carta Europea de los Derechos Fundamentales, y que, además, garanticen que los servicios de inteligencia realicen sus actividades de conformidad con los principios fundamentales, de modo que se correspondan con las disposiciones recogidas en el capítulo 8 del presente informe y, en particular, en el apartado 8.3.4, derivadas del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales;

3. Se pide a los Estados miembros del Consejo de Europa que adopten un protocolo adicional que permita la adhesión de las Comunidades Europeas al Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales o que adopten otro tipo de medidas que excluyan conflictos en relación con la jurisprudencia entre los Tribunales de Estrasburgo y de Luxemburgo;

4. Se insta al Secretario General de las Naciones Unidas a que encargue a la comisión competente de la presentación de propuestas que adapten a la evolución tecnológica el artículo 17 del Pacto Internacional sobre los derechos cívicos y políticos, que protege la vida privada;

5. Se pide a los EE.UU. que firmen el Protocolo adicional al Pacto Internacional sobre los derechos cívicos y políticos, de modo que se puedan presentar ante la Comisión de derechos humanos que se deriva del Convenio las quejas presentadas por particulares contra los EE.UU. por la violación de este Pacto; se pide a las ONG de los EE.UU. pertinentes, en particular a la ACLU (American Civil Liberties Union) y al EPIC (Electronic Privacy Information Center) que ejerzan presiones ante el Gobierno de los EE.UU. en este sentido;

Con respecto a disposiciones legislativas nacionales de protección de los ciudadanos y de las empresas

6. Se insta a todos los Estados miembros a que examinen su propia legislación en relación con la conformidad de las actividades de los servicios de inteligencia con los principios fundamentales;

7. Se pide a los Estados miembros que adopten un nivel de protección común con respecto a las actividades de los servicios de inteligencia que se base en el mayor grado de protección existente en los Estados miembros, ya que, por regla general, los ciudadanos afectados por las actividades de un servicio secreto extranjero son los ciudadanos de otro Estado y, por consiguiente, de otro Estado miembro;

8. Se insta a las instituciones de la UE a que, en caso de que los servicios de inteligencia cooperen en el marco de la PESC, se adopten disposiciones de protección de los ciudadanos europeos de grado suficiente. Por su parte, el Parlamento Europeo, como órgano lógico de control, deberá crear las condiciones necesarias para controlar este ámbito tan sensible, de modo que pueda exigir los derechos de control necesarios de forma realista y responsable;

Con respecto a las medidas jurídicas concretas de lucha contra el espionaje industrial

9. Se pide a los Estados miembros que examinen hasta qué punto la adopción de disposiciones de derecho europeo e internacional podría servir para luchar contra el espionaje industrial y el soborno y, en particular, si sería posible adoptar una normativa en el seno de la OMC que tenga en cuenta el impacto negativo de este tipo de acciones sobre la competencia de modo que, por ejemplo, declare nulos estos contratos;

10. Se pide a los Estados miembros que se comprometan en una declaración común clara a no realizar espionaje industrial entre sí y, de este modo, a dar muestras de su voluntad de respetar el espíritu y la letra del Tratado CE;

En relación con las medidas de aplicación jurídica y su control

11. Hace un llamamiento a los Parlamentos nacionales que no cuentan con ningún tipo de órgano de control parlamentario encargado del control de los servicios de inteligencia a que adopten las medidas necesarias para su creación;

12. Se insta a las comisiones nacionales de control de los servicios de inteligencia que concedan mayor importancia a la protección de la vida privada en el ejercicio de sus competencias en materia de control independientemente de que se trate de controlar a ciudadanos del propio Estado, de otros ciudadanos de la UE o de ciudadanos de terceros países;

13. Se pide a los servicios de inteligencia de los Estados miembros que acepten informaciones procedentes de otros servicios de inteligencia exclusivamente en aquellos casos en que pueda determinar el respeto a las disposiciones previstas en la legislación nacional, ya que los Estados miembros no pueden eximirse de las obligaciones derivadas del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales recurriendo a otros servicios de inteligencia;

14. Se pide a Alemania y al Reino Unido a que en el futuro sólo autoricen la interceptación de las comunicaciones por parte de los servicios de inteligencia de los EE.UU. en su territorio si respetan el Convenio Europeo para la Protección de los Derechos Humanos y Libertades

Fundamentales, es decir, si respetan el principio de proporcionalidad, si su fundamento jurídico es accesible y si sus repercusiones sobre los individuos son previsibles, así como que establezcan un control eficaz, ya que son responsables de que las actividades realizadas por los servicios de inteligencia en su territorio en materia de información, independientemente de que estén autorizadas o que estén únicamente toleradas respetan los derechos humanos ;

En relación con las medidas de impulso de la autoprotección de los ciudadanos y de las empresas

15. Se insta a la Comisión y a los Estados miembros a que desarrollen programas que aumenten el grado de concienciación de los ciudadanos y de las empresas en relación con los problemas relacionados con la seguridad y, al mismo tiempo, a que brindan asistencia práctica para la concepción y la aplicación de sistemas de protección de carácter mundial;

16. Se solicita a la Comisión y a los Estados miembros que adopten medidas adecuadas para impulsar, desarrollar y producir tecnologías y software europeos de codificación, así como, en particular, que apoyen proyectos que tengan como objetivo el desarrollo de software de encriptación de utilización sencilla y cuyo código fuente sea público;

17. Se insta a la Comisión y a los Estados miembros a que impulsen proyectos de software cuyo texto de base sea público, ya que este es el único modo de garantizar que no se incluirán "backdoors" ("open-source software");

18. Se insta a las instituciones europeas y a las administraciones públicas de los Estados miembros a que codifiquen el correo electrónico sistemáticamente para que, a largo plazo, se convierta en la norma;

En relación con otras medidas

19.Se insta a las empresas a que colaboren más estrechamente con los servicios de contraespionaje y que, en particular, les comuniquen los ataques procedentes del exterior con fines de espionaje industrial para aumentar el grado de eficacia de estos servicios;

20. Se pide a la Comisión que presente una propuesta de creación de una oficina europea de asesoramiento dedicada a las cuestiones relacionadas con la seguridad de las informaciones de las empresas que, junto al aumento del grado de sensibilización del problema, también tenga como misión proporcionar ayuda de tipo práctico;

21. Se insta al Parlamento Europeo a que organice un congreso sobre la protección de la vida privada frente a la interceptación de las telecomunicaciones, que no sólo esté dirigido a Europa, para crear una plataforma destinada a las ONG europeas, de los EE.UU. y de otros Estados en la que se puedan debatir aspectos transfronterizos e internacionales y coordinar ámbitos de actuación y procedimientos.