Evaluación de las tecnologías de control político

Steve Wright
Fundación Omega - Manchester

El texto que os ofrecemos a continuación podría parecer una paranoica actualización de “1984”. Pero no se trata de una nueva novela, sino de algo mucho más real. Es un documento de trabajo, resumen de un estudio provisional, elaborado para l@s diputad@s del Parlamento Europeo de septiembre de 1998. La Fundación Omega, autora del estudio, lo tituló:

Avances en las tecnologías de vigilancia

La tecnología de vigilancia puede definirse como los dispositivos o sistemas que pueden vigilar, seguir y evaluar los movimientos de personas, sus propiedades y otros activos. Gran parte de esta tecnología se utiliza para seguir las actividades de disidentes, activistas por los derechos humanos, periodistas, dirigentes estudiantiles, minorías, dirigentes sindicales y opositores políticos. Se ha desarrollado una enorme gama de tecnologías de vigilancia, como los anteojos de visión nocturna, los micrófonos parabólicos para detectar conversaciones realizadas a más de un kilómetro de distancia, versiones de láser, que pueden detectar cualquier conversación desde una ventana cerrada situada en la línea de visión, la cámara estroboscópica danesa Jai, que puede registrar centenares de imágenes en cuestión de segundos, y fotografiar de forma individual a todos los participantes en una manifestación o marcha, y los sistemas de reconocimiento automático de vehículos, que pueden seguir coches por toda una ciudad mediante un sistema cartografiado de información geográfica.

Nuevas tecnologías, concebidas en un principio para los sectores de defensa y espionaje, se han expandido rápidamente tras la guerra fría a las autoridades policiales y aduaneras, así como al sector privado. (...) Hasta la década de los 60, la mayor parte de la vigilancia se realizaba con escasa intervención de la tecnología y era muy costosa, pues requería seguir a los sospechosos de un lugar a otro, utilizando hasta 6 personas en equipos de dos, trabajando en tres turnos de ocho horas. Todo el material y los contactos recogidos debían mecanografiarse y archivarse, con pocas posibilidades de comprobación cruzada. Hasta la vigilancia electrónica requería gran cantidad de personal. Por ejemplo, la policía de Alemania Oriental empleaba a 500.000 informadores secretos, 10.000 de los cuales eran necesarios tan sólo para escuchar y transcribir las llamadas telefónicas de los ciudadanos.

En la década de los 80, comenzaron a aparecer nuevas formas de vigilancia electrónica, muchas de las cuales se orientaban hacia la automatización de la interceptación de las comunicaciones. Esta tendencia se vio incrementada en los Estados Unidos en la década de los 90 gracias a un aumento de la financiación del Gobierno al final de la guerra fría, momento en que los organismos de defensa y espionaje cambiaron su centro de interés y asumieron nuevas misiones para justificar sus presupuestos, transfiriendo sus tecnologías a ciertas aplicaciones policiales y aduaneras, como las operaciones contra la droga o el terrorismo. En 1993, los departamentos de defensa y de justicia de los Estados Unidos firmaron por separado documentos de acuerdo para realizar «operaciones distintas de las bélicas y policiales» con el fin de facilitar el desarrollo conjunto y la utilización en común de la tecnología.

Según David Banisar de Privacy International, «para contrarrestar las reducciones de contratos militares que comenzaron en la década de los 80, las empresas de informática y electrónica se expanden en nuevos mercados, en su país y en el extranjero, con equipos desarrollados en un principio para fines militares. Empresas como E Systems, Electronic Data Systems y Texas Instruments venden sistemas informáticos avanzados y equipos de vigilancia a gobiernos estatales y locales que los utilizan para funciones policiales, control de fronteras y administración de subsidios sociales». Lo que la policía secreta de Alemania oriental sólo pudo soñar se está rápidamente convirtiendo en una realidad en el mundo libre.

Redes de vigilancia por circuito cerrado de televisión (CCTV)

En realidad, la técnica de la vigilancia visual ha cambiado de forma espectacular en los años recientes Desde luego, los agentes de policía y de espionaje siguen fotografiando manifestaciones y personas de interés, pero cada vez hay más posibilidades de almacenamiento e investigación de dichas imágenes. Los actuales procesos de ultra-miniaturización permiten que estos dispositivos sean virtualmente imposibles de detectar (...)

La actitud hacia las redes de cámaras de CCTV es muy diferente en el interior de la Unión Europea, desde la posición de Dinamarca, donde dichas cámaras están prohibidas, hasta la posición del Reino Unido, donde existen centenares de redes de

CCTV. (...) Dado que el material de estos sistemas puede modificarse sin dejar rastro, la Directiva europea sobre protección de datos necesita aplicarse a través de legislación primaria que clarifique la ley en su aplicación al CCTV, con el fin de evitar la confusión, tanto entre quienes controlan la información procedente de CCTV como entre los ciudadanos, a quienes se refiere dicha información. (...)

Sistemas algorítmicos de vigilancia

La revolución en la vigilancia urbana alcanzará la próxima generación de control una vez se disponga de un sistema fiable para reconocer los rostros. En un principio, se introducirá en lugares fijos, como puertas de entrada, aduanas, accesos de seguridad, etc., para permitir que se realice un reconocimiento facial total normalizado. El estudio provisional preveía que en la primera mitad del siglo XXI, el reconocimiento facial por CCTV seria una realidad y los países con infraestructuras de CCTV considerarían esta tecnología como una adición natural. De hecho, la empresa estadounidense Software and Systems ha ensayado un sistema en Londres que puede registrar una multitud, y comparar los rostros con una base de datos de imágenes situada en un ordenador remoto. Nos encontramos en el principio de una revolución en la «vigilancia algorítmica»: análisis efectivo de la información mediante algoritmos complejos que permiten el reconocimiento y el seguimiento automáticos. Esta automatización no sólo amplía la red de vigilancia, sino que también estrecha sus mallas (Véase Norris, C. y otros, 1998).

De forma similar, se han desarrollado sistemas de reconocimiento de vehículos que pueden identificar el número de matrícula de un automóvil y después seguirlo por toda una ciudad utilizando un sistema informatizado de información geográfica. Estos sistemas se comercializan en la actualidad; por ejemplo, el sistema Talon, presentado en 1994 por la empresa del Reino Unido Racal al precio de 2.000 libras (500.000 ptas.) por unidad. El sistema está preparado para reconocer las matrículas sobre la base de la tecnología de redes neurales desarrollada por Cambridge Neurodynamics, y puede ver tanto por la noche como por el día. En un principio, se ha utilizado para el control de tráfico, pero recientemente se ha adaptado su función para incluir la vigilancia de seguridad y se ha incorporado al «círculo de acero» alrededor de Londres. El sistema puede registrar todos los vehículos que han entrado o salido del cordón en una fecha dada.

Es importante establecer orientaciones y códigos de conducta claros para estas innovaciones tecnológicas, muy por delante de la revolución digital y que ofrecen nuevas e imprevisibles oportunidades de comparar, analizar, reconocer y almacenar estas imágenes visuales. Ya los sistemas multifunción de gestión de tráfico como «Traffic Master» (que utiliza sistemas de reconocimiento de vehículos para cartografiar y cuantificar la congestión) facilitan una arquitectura nacional de vigilancia. Es necesario que la reglamentación se base en solidos principios de protección de datos y tenga en cuenta el artículo 15 de la Directiva europea de 1995 (...), que establece lo siguiente: «Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base en un tratamiento automatizado de datos». (...)

Estos sistemas de vigilancia suscitan importantes cuestiones de responsabilidad, en particular cuando se transfieren a regímenes autoritarios. Siemens Plessey vendió las cámaras que se utilizaron en la plaza Tiananmen como sistemas avanzados de control de tráfico. Y después de la matanza de estudiantes de 1989 se produjo una caza de brujas en que las autoridades torturaron e interrogaron a miles de personas para localizar a los subversivos. El sistema de vigilancia Scoot, con cámaras Pelco fabricadas en Estados Unidos, se utilizó para grabar fielmente las protestas. Las imágenes se emitieron repetidamente por la televisión china, ofreciendo una recompensa por la información, con el resultado de que se identificó a casi todos los transgresores. Una vez más, la responsabilidad democrática es el único criterio que distingue a un moderno sistema de control de tráfico de una tecnologia avanzada para la captura de disidentes. Empresas extranjeras exportan sistemas de control de tráfico a Lhasa, en el Tibet, aunque en Lhasa no existan aún problemas de control de tráfico. Puede que en estos casos el problema consista en una culpable falta de imaginación.

Dispositivos de escucha y grabación

Se ha desarrollado una amplia gama de dispositivos de escucha y grabación con el fin de registrar conversaciones e interceptar el tráfico de telecomunicaciones. En los últimos años la extendida práctica de interceptación legal e ilegal de las comunicaciones y la colocación de «escuchas» ha constituido un problema en muchos Estados europeos. Sin embargo, la colocación de micrófonos ilegales es una tecnología del pasado. Los espías modernos pueden comprar ordenadores portátiles adaptados especialmente y sintonizar con facilidad todos los teléfonos móviles en funcionamiento en la zona simplemente colocando el cursor sobre el número. La máquina puede incluso buscar números «de interés» y comprobar si están activos. Sin embargo, estas escuchas y grabaciones palidecen hasta la insignificancia frente a las redes de interceptación nacionales e internacionales gestionadas por el Estado.

Redes nacionales e internacionales de interceptación de las comunicaciones

El estudio provisional detalla los sistemas globales de vigilancia que facilitan la supervisión masiva de todas las telecomunicaciones, incluyendo las comunicaciones telefónicas, por correo electrónico y por fax de los ciudadanos, los políticos, los sindicalistas y las empresas por igual. En los últimos años se ha producido un giro político en cuanto al objetivo de la vigilancia. En vez de investigar la delincuencia (que es reactiva), las autoridades policiales y aduaneras siguen cada vez más a determinadas clases sociales y razas que viven en zonas marcadas antes de que se cometa el delito; se trata de una forma de investigación policial preventiva, denominada "reserva de datos", basada en modelos militares de recogida de enormes cantidades de información de bajo nivel.

Sin codificar, los modernos sistemas de comunicaciones son virtualmente transparentes para los equipos avanzados de interceptación que pueden utilizarse para la escucha. El estudio provisional también explica cómo los teléfonos móviles tienen parámetros integrados de control y seguimiento a los que pueden tener acceso la policía y las agencias de espionaje. Por ejemplo, la tecnología digital necesaria para localizar a los usuarios de teléfonos móviles que reciben llamadas significa que todos los teléfonos móviles de un país, cuando los activan, constituyen pequeños dispositivos de seguimiento, que indican la situación de sus propietarios en cualquier momento, información que se almacena en el ordenador de la empresa.

Por ejemplo, la policía suiza ha seguido en secreto la situación de usuarios de teléfonos móviles a partir del ordenador de la empresa suministradora del servicio, Swisscom, que, según el periódico Sonntags Zeitung, tenía almacenados los movimientos de más de un millón de abonados a una escala de unos centenares de metros, y por un periodo que abarcaba al menos los seis meses anteriores. Sin embargo, de todos los avances a que se refiere el estudio provisional, la sección que examina (...) el acceso y la facilidad de la Agencia Nacional de Seguridad de los Estados Unidos para interceptar todas las telecomunicaciones europeas es la que produjo la mayor preocupación. Aunque nadie negó la utilidad de tales redes en las operaciones antiterroristas y la lucha contra el tráfico de drogas, el blanqueo de dinero y el tráfico de armas, se manifestó la alarma por la escala de la red extranjera de interceptación identificada en el estudio, y por si la legislación y salvaguardas en cuanto a la protección de datos y de la intimidad existentes en los Estados miembros serían suficientes para proteger la confidencialidad entre los ciudadanos y empresas de la UE, y de estos con los terceros países.

(...) Merece la pena clarificar algunos de los problemas relacionados con la vigilancia electrónica transatlántica, así como facilitar una breve historia y puesta al día de los acontecimientos desde la publicación del informe provisional en enero de 1998. Existen fundamentalmente dos sistemas separados, a saber:

(i) El sistema RU/EEUU, que incluye las actividades de las agencias de espionaje militar como NSA-CLA en los Estados Unidos, y que incluyen las actividades de GCHQ y MI6 del Reino Unido, y que funcionan en un sistema conocido como ECHELON.

(ii) El sistema UE-FBI, que enlaza a diversas autoridades policiales y aduaneras, como el FBI, la policía, las aduanas, la inmigración y la seguridad interior.

(...) En términos de inteligencia, se trata de dos «comunidades» distintas; vale la pena examinar brevemente las actividades de ambos sistemas por separado, incluyendo ECHELON, codificación, vigilancia UE-FBI con nuevos interfaces, por ejemplo, para el acceso a los suministradores de Internet y a las bases de datos de otras agencias.

Interceptación por la NSA de todas las telecomunicaciones de la UE

El estudio provisional indicaba que en Europa, todas las comunicaciones por correo electrónico, teléfono y fax se interceptan como cuestión de rutina por la Agencia Nacional de Seguridad de los Estados Unidos, y que la información se transfiere desde el continente europeo a través del nodo estratégico de Londres y después por satélite a Fort Meade, en Maryland, a través del nodo crucial de Menwith Hill, en los páramos del norte de York, en el Reino Unido.

El sistema fue descubierto por primera vez en la década de los 70 por un grupo de investigadores del Reino Unido (Campbell, 1981). Un reciente trabajo de Nicky Hager, «Secret Power» (Poder secreto) (Hager, 1996) contiene los datos más exhaustivos hasta la fecha sobre el proyecto llamado ECHELON. Hager entrevistó a más de 50 personas relacionadas con el espionaje para documentar un sistema de vigilancia global que se extiende por todo el mundo y constituye un sistema orientado sobre todos los satélites Intelsat claves que se utilizan para transmitir la mayor parte de las llamadas telefónicas, comunicaciones

Internet, correo electrónico, fax y télex por satélite en todo el mundo. Las bases se encuentran en Sugar Grove y Yakima (Estados Unidos), en Waihopai (Nueva Zelanda), en Geraldton (Australia), en Hong Kong y en Morwenstow (Reino Unido).

El sistema ECHELON forma parte del sistema RU/EEUU pero a diferencia de muchos de los sistemas electrónicos de espionaje desarrollados durante la guerra fría, ECHELON está diseñado para objetivos fundamentalmente no militares: gobiernos, organizaciones y empresas en prácticamente todos los países. El sistema ECHELON funciona interceptando de forma indiscriminada enormes cantidades de comunicaciones, seleccionando posteriormente lo que es de valor mediante el uso de ayudas de inteligencia artificial, como Memex, para encontrar palabras clave. Cinco países comparten los resultados con los Estados Unidos, que es el socio principal, según el acuerdo RU/EEUU de 1945: Reino Unido, Canadá, Nueva Zelanda y Australia actúan en gran medida como suministradores de información y subordinados. Cada uno de los cinco centros facilita a los otros cuatro «diccionarios» de palabras clave, frases, personas y lugares a «marcar», y la información interceptada marcada se envía directamente al país solicitante. Aunque se reúne mucha información sobre posibles terroristas, existe también abundante información económica, en particular un intenso control de todos los países que participan en las negociaciones del GATT. Pero Hager descubrió que, con diferencia, la principal prioridad de este sistema seguía siendo el espionaje político y militar aplicable a sus intereses más amplios.

Hager cita a «agentes de espionaje con altos cargos», que declararon a The Observer en Londres «Pensamos que no podemos seguir callados ante lo que consideramos como un grave desafuero y negligencia en la institución en la que trabajamos». Como ejemplo, señalaron la interceptación por GCHQ de tres actividades altruistas, entre ellas Amnistía Internacional y Christian Aid. «En cualquier momento GCHQ puede intervenir sus comunicaciones para responder a una petición de rutina», manifestó la fuente de GCHQ. En el caso de intervención telefónica, el procedimiento se conoce como Mantis. En el caso de los télex se llama Mayfly. Al teclear un código relacionado con la ayuda al tercer mundo, la fuente pudo demostrar que existían referencias («fixes») de telex en estas tres organizaciones. Sin ningún sistema de control, es difícil descubrir los criterios que determinan quién puede sustraerse a la vigilancia.

Desde luego, tras la publicación del estudio provisional, los periodistas han argumentado que ECHELON ha beneficiado a las empresas estadounidenses relacionadas con el tráfico de armas y ha reforzado la posición de Washington en conversaciones cruciales de la Organización Mundial de Comercio con Europa durante las diferencias de 1995 sobre las exportaciones de repuestos de automóviles. Según el Financial Mail on Sunday, «las palabras clave identificadas por los expertos de Estados Unidos incluyen los nombres de las organizaciones comerciales intergubernamentales y consorcios de empresas que licitan contra empresas estadounidenses. En la lista se encuentra la palabra «block» para identificar las comunicaciones sobre depósitos de petróleo en alta mar en las zonas en que el lecho marino aún no se ha dividido en bloques de prospección» (...) «también se ha indicado que en 1990 los Estados Unidos lograron acceso a negociaciones secretas y persuadieron a Indonesia de que incluyera al gigante estadounidense AT&T en un negocio de telecomunicaciones de miles de millones de dólares, que en un momento dado, se destinaba por entero a la empresa japonesa NEC».

El Sunday Times (11 de mayo de 1998) informó que al principio de las actividades en Menwith Hill (estación de la NSA F83) en el norte de Yorkshire (Reino Unido), se les asignó la tarea de interceptar el tráfico de portador alquilado internacional (ILC), consistente, en lo fundamental, en comunicaciones comerciales ordinarias. El personal de esta instalación aumentó desde 400 en la década de los 80 hasta más de 1.400 en la actualidad, contando además con 370 personas procedentes del Ministerio de Defensa. El Sunday Times también informaba sobre acusaciones en el sentido de que se habían interceptado conversaciones entre la empresa alemana Volkswagen y General Motors, y Francia ha protestado porque Thomson-CSF, empresa francesa de electrónica, perdió un contrato de 1.400 millones de dólares para el suministro a Brasil de un sistema de radar debido a que los estadounidenses interceptaron detalles de las negociaciones, que transmitieron a la empresa estadounidense Raytheon, que posteriormente obtuvo el contrato.

Otra acusación es que Airbus Industrie perdió un contrato por un importe de 1.000 millones de dólares a favor de Boeing y McDonnell Douglas debido a la interceptación de información por el espionaje estadounidense. Otros periódicos, como Libération (21 de abril de 1998) e Il Mondo (20 de marzo de 1998) identifican a esta red como una red de espionaje anglosajona a causa del eje Estados Unidos/Reino Unido. Privacy International va más lejos. Aunque reconoce que, estrictamente hablando, ni la Comisión ni el Parlamento Europeo tienen competencia para regular o intervenir en materia de seguridad tienen una responsabilidad en su armonización en el conjunto de la Unión.

Según Privacy International, es probable que el Reino Unido encuentre que sus lazos en virtud de la «relación especial» sean incompatibles con sus obligaciones en virtud del Tratado de Maastricht, cuyo Título V establece que «los Estados miembros se informarán mutuamente y se concertarán en el seno del Consejo sobre cualquier cuestión de política exterior y de seguridad

que revista un interés general, a fin de garantizar que su influencia combinada se ejerza del modo más eficaz mediante una acción concertada y convergente». Sin embargo, de acuerdo con las condiciones de la relación especial, el Reino Unido no puede consultar abiertamente a sus socios europeos. La situación se complica aún más por las acusaciones en sentido contrario de la revista francesa Le Point, en el sentido de que los franceses espían de forma sistemática el tráfico por teléfono y cable de los Estados Unidos y otros países aliados a través del satélite espía Helios 1A (The Times, 17 de junio de 1995).

Aunque no más de la mitad de estas acusaciones fuesen ciertas, el Parlamento Europeo debería actuar para garantizar que estos potentes sistemas de vigilancia funcionen dentro de un consenso más democrático, ahora que la guerra fría ha terminado. Está claro que las políticas internacionales de los Estados miembros de la Unión Europea no siempre son congruentes con las de los Estados Unidos, y, en términos comerciales, el espionaje es el espionaje. Ninguna autoridad de los Estados Unidos permitiría que una red de espionaje similar de la UE funcionase en su territorio sin estrictas limitaciones, en caso de permitirla. Tras un completo examen de las repercusiones de las operaciones de estas redes, se recomienda al Parlamento Europeo que establezca un adecuado control independiente y procedimientos de supervisión, y que se impida cualquier esfuerzo de ilegalizar la codificación por parte de cualquier ciudadano de la UE, salvo que se hayan creado estos sistemas de control y responsabilidad democráticos.

Sistema global de vigilancia de las telecomunicaciones UE-FBI

Gran parte de la documentación e investigación necesarias para sacar a la luz pública la historia, la estructura, el papel y la función del convenio UE-FBI para legitimar la vigilancia electrónica global ha sido facilitada por Statewatch, la muy respetada organización del Reino Unido de investigación y defensa de las libertades públicas.

Statewatch ha descrito con detalle la firma de la Agenda transatlántica en Madrid en la cumbre UE-EE.UU. del 3 de diciembre de 1995, parte de la cual fue el plan de acción conjunto UE-EE.UU., y posteriormente ha analizado estos esfuerzos como un continuo intento de volver a definir la Alianza Atlántica en la era posterior a la guerra fría, argumento que cada vez se utiliza con más frecuencia para justificar los esfuerzos de las autoridades de seguridad interior para asumir más funciones de policía en Europa. Statewatch señala que el primer plan de vigilancia conjunto «fuera del área» no se examinó en la reunión de justicia e interior, sino que su núcleo fundamental se adoptó como punto A (sin debate), en el sorprendente foro del Consejo de Pesca del 20 de diciembre de 1996.

En febrero de 1997, Statewatch informó que la UE había acordado en secreto la creación de una red internacional de intervenciones telefónicas a través de una red secreta de comités creados de acuerdo con el «tercer pilar» del Tratado de Maastricht, que se refiere a la cooperación para la protección de la ley y el orden público. Los puntos fundamentales del plan se describen en un memorándum de acuerdo, firmado por Estados de la UE en 1995 (ENFOPOL 112 10037/95 25.10.95) y que se mantiene secreto Según informa The Guardian (25.2.97), este documento refleja la preocupación existente en agencias europeas de espionaje en caso de que las modernas tecnologías les impidan la intervención de las comunicaciones privadas.

«Los países de la UE», dice, «deberían acordar estándares internacionales de intervención establecidos a un nivel que garantizase que los organismos gubernamentales pudieran romper la codificación o mezcla de las palabras». Informes oficiales indican que los Gobiernos de la UE estuvieron de acuerdo en cooperar estrechamente con el FBI en Washington. Sin embargo, actas anteriores de estas reuniones indican que la primera iniciativa procedía de Washington. Según Statewatch, los suministradores de redes y servicios de la UE se verán obligados a instalar sistemas «interceptables», y a poner bajo vigilancia a cualquier persona o grupo siempre que reciban una orden de interceptación.

Dichos planes nunca se han transmitido para su examen a un Gobierno europeo, ni a la Comisión de Libertades Públicas del Parlamento Europeo, a pesar de los evidentes problemas de libertades públicas que plantea un sistema tan incontrolado. La decisión de ir adelante simplemente se adopto en secreto mediante «procedimiento escrito» a través de un intercambio de télex entre los 15 Gobiernos de la UE. Statewatch indica que el plan de vigilancia global UE-FBI ya se desarrollaba fuera del «tercer pilar».

En términos prácticos, esto significa que el plan lo está poniendo en marcha un grupo de veinte países: los 15 Estados miembros de la UE, junto con Estados Unidos, Australia, Canadá, Noruega y Nueva Zelanda. Este grupo de 20 no debe responder ante el Consejo de Ministros de Justicia e Interior ni ante el Parlamento Europeo, ni ante los parlamentos nacionales. No se dice nada acerca de la financiación de este sistema, pero un informe elaborado por el Gobierno alemán calcula que sólo la parte correspondiente a telefonía móvil del paquete costará 4.000 millones de marcos.

Statewatch concluye que «es el interface del sistema ECHELON y su posible desarrollo sobre las llamadas telefónicas, combinado con la normalización de centros de comunicación y equipos "interceptables", financiados por la UE y los Estados Unidos lo que constituye una verdadera amenaza global sobre la que no existe control alguno, ni jurídico ni democrático» (Comunicado de prensa, 25.2.97). En muchos aspectos, somos testigos de reuniones de agentes de un nuevo estado global de espionaje militar. Es muy difícil que cualquiera pueda tener una imagen completa de lo que se decide en las reuniones ejecutivas que ponen en marcha esta «Agenda transatlántica». Aunque Statewatch logró una decisión del Defensor del Pueblo favorable al acceso a los documentos, con el fundamento de que el Consejo de Ministros no aplicaba el código de acceso, por el momento el Consejo sigue negando el acceso a los órdenes del día.(...) Es posible que los diputados al Parlamento Europeo quieran examinar las siguientes opciones políticas:

Opciones políticas

1) Debe encargarse una serie de estudios más detallados sobre las repercusiones sociales, políticas comerciales y constitucionales de las redes mundiales de vigilancia electrónica (...) para dar una base de información a la futura política de la UE (...) Estos estudios podrían versar sobre:

(a) Los problemas constitucionales que plantea la facilidad de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos para interceptar todas las telecomunicaciones europeas,(...) así como el conjunto de la cuestión del uso de esta red para el espionaje comercial y político automatizado.

(b) Las repercusiones sociales y políticas del sistema mundial de vigilancia UE-FBI, su creciente acceso a nuevos medios de comunicación, incluyendo el correo electrónico y su creciente expansión en nuevos países, así como todos los problemas financieros y constitucionales relacionados.

(c) La estructura, la función y las competencias de un organismo de supervisión a nivel de la UE, independiente del Parlamento Europeo, que podría crearse para supervisar y controlar las actividades de todos los organismos que se ocupan de la interceptación de las telecomunicaciones dentro de Europa.

2) El Parlamento Europeo tiene la opción de instar a que se rechacen las propuestas de Estados Unidos de hacer accesibles los mensajes privados, a través de Internet, a los servicios de espionaje de los Estados Unidos. (...) Estas repercusiones afectan a los derechos cívicos y humanos de los ciudadanos europeos y a los derechos comerciales de las empresas a funcionar dentro de la ley, sin una vigilancia injustificada por parte de organismos de espionaje que funcionan de acuerdo con sus competidores multinacionales.

extraído de la revista Ekintza Zuzena nº26, 2000
http://www.nodo50.org/ekintza/article.php3?id_article=216