

NUEVAS TECNOLOGÍAS PARA EL CONTROL POLÍTICO *

Por Catherine Mordos

El caso Pinochet ha vuelto a poner de actualidad las investigaciones en torno a los métodos utilizados por las dictaduras para mantener su poder sobre la ciudadanía. Sin embargo, no sólo estos regímenes autoritarios echan mano de sistemas que, si no ilegales, cuando menos se encuentran fuera del control político o judicial. Dos documentos hechos públicos recientemente, un estudio oficial del Parlamento Europeo y un trabajo basado en informes desclasificados del Gobierno norteamericano, revelan el uso masivo de nuevas tecnologías, aplicadas a la vigilancia y manipulación social y política de la población civil. Unas tecnologías que, por su misma novedad, escapan a cualquier regulación por parte de los poderes ejecutivos de los países, incluso de los más democráticos, como la propia Europa.

Salir de un avión en cualquier aeropuerto, una simple conversación por el teléfono móvil o incluso asistir a una manifestación de cualquier signo puede significar, para cada ciudadano europeo, la posibilidad de ser identificado, de forma inmediata, fichado y controlado. Y esto no ocurre en un país bajo régimen dictatorial, sino en nuestras propias democracias liberales de la muy civilizada Europa. Las nuevas tecnologías de la comunicación y la informática no sólo están permitiendo la aparición de legiones de sofisticados ordenadores y teléfonos cada vez más refinados, sino que también sirven para tener bajo control a la

* Originalmente Publicado en la revista *El Siglo*, de Madrid (España) en su número 351 de 7 feb 99

población civil, dejando atrás, por puro obsoletos, antiguos métodos de represión violenta propios de las dictaduras.

Estas nuevas tecnologías, como la usada en el sistema Echelon de vigilancia y seguimiento masivo de población civil, sólo son conocidas por un sector muy minoritario de la sociedad, y son controladas y usadas por grupos aún más reducidos de responsables. De hecho, hasta la década de los setenta esta tecnología sólo estaba en manos de los militares, por lo que su uso estaba restringido, en la mayoría de los casos, a conflictos internacionales o a situaciones de dictaduras militares. Sin embargo, a partir de ese momento han sido los investigadores y las empresas civiles los que han tomado las riendas de los avances científicos, que a su vez han empezado a ser usados por los poderes civiles para controlar, vigilar y, en su caso, manipular a la población.

A estas alturas el único país que tiene la capacidad y los medios suficientes como para liderar este extraño sector es Estados Unidos, aunque otros muchos países, incluidos los de la Unión Europea, se aprovechan en buena medida de sus ventajas para sus propios intereses. La imposibilidad de controlar el uso de estos nuevos sistemas viene dado, en muchos casos, por el hecho de que en la actualidad la mayoría de las comunicaciones entre los ciudadanos se hacen vía satélite, es decir, fuera del espacio cubierto y protegido por la legislación de cada país. Y ahí se plantea la duda. ¿A quién le corresponde controlar y limitar las actividades de los aparatos instalados fuera de nuestra atmósfera? Hoy por hoy, a nadie, salvo al propio responsable de su instalación, que goza de total libertad en la utilización de su aparato.

Así pues, una de las conclusiones más claras de estos dos estudios señala que, hoy en día, no se requiere la intervención de ningún juez, ni existe ley alguna que regule la interceptación de

llamadas efectuadas a o desde teléfonos móviles vía satélite, es decir, basados en tecnología GSM.

El secretismo que rodea el uso de nuevas tecnologías para el control político y social de la población tan sólo se ha roto muy recientemente, gracias en parte a ese traslado de la utilización de estos nuevos sistemas al sector civil.

Estos dos documentos, de carácter semioficial y difundidos hace poco a través de Internet, revelan datos que a veces parecen más propios de la ciencia ficción pero que están basados en estudios rigurosos efectuados por expertos de reconocido prestigio y avalados, en el caso del primer trabajo, por una institución como el Parlamento Europeo. Así, el primer documento que aquí resumimos, un STOA (es decir, un trabajo de asesoramiento científico) número PE 166 499, es una investigación realizada a petición del propio Parlamento, bajo el título de An Apraisal of the technology of political control (Una aproximación a las tecnologías de control político).

Su autor material es Steve Wright, un afamado experto, activista de derechos humanos, perteneciente a la organización Omega, dedicada a este tipo de investigaciones sobre la violación de las libertades civiles y ha contado con la ayuda y el asesoramiento de un amplio grupo de universidades, organismos y asociaciones. Y aunque el extenso documento no refleja, tal y como se advierte, el parecer del Parlamento Europeo, sí sirve como base de trabajo, lo cual supone una garantía.

En este estudio, el propio índice ya resulta muy revelador. En su exposición de objetivos señala que, entre otros, los objetivos de este informe consisten en "proveer a los miembros del Parlamento Europeo con una guía de los recientes adelantos tecnológicos destinados al control político", además de "identificar, analizar y describir el actual estado" de estos avances. En el

estudio se hace referencia a las implicaciones que conlleva la "globalización y la militarización del equipamiento (utilizado por las policías", es decir, al hecho de que el armamento militar pasa a ser de uso policial, y a la "convergencia de los sistemas de control desplegados en todo el mundo". Asimismo, estudia "los desarrollos en materia de tecnología de vigilancia y control (incluyendo la emergencia de nuevas formas de redes de interceptación de comunicaciones en el ámbito local, nacional e internacional -vía satélite-", o "innovaciones en armamento de control de masas (incluyendo la evolución de una segunda generación de las llamadas armas no letales" en los laboratorios nucleares de Estados Unidos)". Sobre todo, en los departamentos de análisis de control de población civil en caso de guerra nuclear de esos laboratorios.

Una de las primeras conclusiones a las que llega el estudio, y sin duda la más escalofriante, es acerca de la existencia del "uso masivo de redes de interceptación de las comunicaciones, desarrolladas sobre el espacio europeo, con las que se identifican comunicaciones de teléfonos, fax, correo electrónico de ciudadanos privados, políticos, sindicalistas y compañías comerciales". Esta red global de vigilancia y seguimiento, añade el documento, que es "parcialmente controlada por servicios de inteligencia de fuera de Europa, no tiene ningún control parlamentario ni se ha discutido ni su rol ni su función en ningún momento de la historia". En otro apartado del texto se asegura que en el espacio judicial europeo todo esto significa la interceptación del 100% de las comunicaciones.

Entre los sistemas de control a los que hace referencia, con multitud de detalles, incluidas en ocasiones empresas fabricantes, este documento se encuentran, por ejemplo, la existencia de ordenadores, con sus correspondientes programas de reconocimiento y seguimiento de voz. Es decir, que se dedican a

interceptar las comunicaciones en los satélites, esto es, fuera del espacio judicial de cualquier país, son capaces de reconocer la voz de una persona y seguir esa voz a través de las comunicaciones en todo el mundo. Con esto, no se necesita saber quién es la persona a la que se vigila, ni saber su número de teléfono desde donde llama, sino que reconoce el tono de su voz, lo que en términos científicos se conoce como el diagrama fonético. Este tipo de programas permite, además, el análisis sintáctico de los discursos. Esto es, reconoce el tema que se está tratando en una conversación, incluso si se usan subterfugios.

Este complejo sistema permite hacer el seguimiento mediante el programa Taurus, es decir, por medio de palabras clave que se refieren al tema que interese controlar. Un ejemplo: alguien quiere vigilar a todos los activistas antinucleares de un país. Basta con que el responsable marque como palabras clave "central" y "nuclear" para tener bajo su control todas las conversaciones que se producen en todo el mundo, incluido nuestro país, sobre este tema. Estas conversaciones, posteriormente, pasarán a ser analizadas por los ordenadores, para saber quién habla con quién. Se pueden además cruzar los temas, es decir, averiguar quién habla de energía nuclear y además menciona el nombre de algún grupo ecologista determinado.

Se cita en este terreno el sistema Memex, que hace posible el construir, en tiempo real, una imagen virtual de cualquier persona y que ofrece el listado de todos los accesos electrónicos de las últimas horas, a través de las tarjetas de pago, registros bancarios, transacciones por caja, etc. De esta forma, con un sistema inteligente, se pueden seguir todos los movimientos de una persona e interceptar sus conversaciones vía satélite, sabiendo en todo momento dónde se encuentra y qué está haciendo. En este sentido, hay que recordar que los teléfonos

móviles, todos, sirven para la localización de sus usuarios sobre plano, con un error de unos pocos metros.

En el terreno de la identificación de personas, los adelantos, ya a la venta, son pasmosos. Así, han quedado atrás viejas técnicas como el cotejo de huellas digitales o la simple foto. Ahora, los más modernos utilizan sistemas de reconocimiento de personas a través de los genes -basta con una muestra de pelo, recogida, por ejemplo, de la silla donde se sentó la persona buscada- o del olor personal. Los olores (las feromonas), en este sentido, pueden ser plasmados mediante diagramas, que a su vez pueden ser tratados como cualquier otra información en un ordenador. Cada persona tiene, pues, su propio diagrama de olor, que puede servir para identificarle a distancia, con tanta seguridad como una foto o unas huellas digitales.

Los ordenadores, junto con las telecomunicaciones, han sido los sectores que mayores adelantos científicos han incorporado. Así, en informática, hay sistemas llamados "redes neuronales de semi inteligencia". Se trata de una tecnología relacionada con la robótica, con software de sistemas expertos, que permite remplazar al personal en determinadas zonas de control, por ejemplo fronteras. Procede, en su mayoría, de investigaciones desarrolladas por Israel, por una lado, y Gran Bretaña destinada a controlar el problema irlandés, por el otro. Este sistema automático de control de fronteras, a través de cámaras de vídeo, identifica personas, determina lo que hace e incluso activa disparos automáticos. Hay satélites capaces de reconocer un objeto de dos centímetros, ponerlo en tres dimensiones e identificarlo, o incluso de reconocer personas. (Aunque no figura en el informe, el origen de los terroristas de usar pasamontañas procede de los palestinos, que se dieron cuenta de que eran sistemáticamente identificados en la frontera. O el caso de varios militantes de la banda terrorista alemana Baäder Meinhoff, que

fueron identificados por una cámara de vídeo instalada a la salida de un avión. Este sistema de control es hoy práctica común en todos los aeropuertos.)

También hay adelantos notables en materia de control físico de movimientos masivos de población, ya sean desplazados, manifestaciones o cualquier otro tipo de concentraciones humanas. Así, a este material se le denomina menos letal, y aunque tiene su origen en las tradicionales pelotas de goma y gases lacrimógenos, llegan a un grado de sofisticación espeluznante. Están, hoy en día, a la venta libre en el mercado, y con cierto éxito ya que se siguen fabricando materiales como balas -utilizables en cualquier tipo de fusil de uso policial corriente- que producen, al liberar los gases spray que llevan incorporados, efectos como pérdida de memoria temporal, sueño, vómitos o pérdida de control corporal al puñado de personas que se encuentran en las inmediaciones de la zona de impacto (ver recuadro adjunto). Otro tipo de proyectiles están diseñados específicamente para producir, al impactar en la cabeza de los blancos humanos, conmociones cerebrales que dejan fuera de juego, durante unas horas, al objetivo, sin causar daños irreparables. Para conseguir estos resultados, apunta el informe, se han hecho estudios exhaustivos sobre la resistencia del cráneo humano a los impactos. Todo esto se complementa con modernos ordenadores, que son capaces de fotografiar cada uno de los participantes en la manifestación o concentración, identificarlos en tiempo real y determinar -en su caso neutralizándolos con las armas no letales- quiénes son los líderes. Asimismo, resulta fácil determinar las vías de salida de una manifestación, por ejemplo.

Existen también, y son utilizados en el ámbito de control de población, sofisticados vehículos de reconocimiento de voz. En ellos viajan expertos en comunicaciones que, con los medios

con que cuenta el vehículo, pueden interceptar las conversaciones telefónicas que mantienen los habitantes, por ejemplo, de una localidad determinada. El ordenador de a bordo, por sistemas de reconocimiento de voz, de análisis sintáctico y lingüístico -que permite, con sólo oír a una persona, determinar de dónde procede y una parte de su historial- y de identificación de ficheros ya existentes, es capaz de determinar, otro ejemplo, la red real de activismo social. Lo que los expertos llaman "los nodos interpersonales", y determinar el "camino crítico" para destruir esa red. Dicho de forma más sencilla, el ordenador identifica, mediante la voz, a los líderes de opinión - que no tienen por qué ser los dirigentes oficiales-, con quién hablan y cuáles son las relaciones que mantienen unas personas con otras. De esta forma, ofrece, en 24 ó 48 horas, una lista concreta y cerrada de nombres. Estas personas, ni una más ni una menos, son las que hay que neutralizar para desmembrar socialmente la población y cortar cualquier movimiento que se haya creado en su seno.

Este equipamiento de última generación puede y de hecho es utilizado por lo que el estudio llama "cuerpos paramilitares" y "parapoliciales" (en el sentido de cuerpos especiales) y que designan a grupos como, se indica en el informe, la Gendarmerie Nationale francesa, los Carabinieri en Italia, el Granz Schutz Gruppe, en Alemania, las Special Patrol Group en Gran Bretaña o cuerpos federales norteamericanos, como la DEA, FBI o BATF. El informe aporta, a este respecto, un elemento de reflexión, al apuntar que la tecnología actualmente existente permite, por primera vez, su uso por parte, por ejemplo, de un policía sin tener que pedir ningún tipo de permiso ni a su jefe ni, por supuesto, a ninguna autoridad judicial. Esto ocurre con el libre acceso a bases de datos y ficheros sobre personas.

En relación a los ordenadores dedicados a elaborar listas de personas que, con su desaparición, permiten el control total de una población, el informe cita, por primera vez, un caso concreto. Se trata del testimonio de un coronel guatemalteco que relata cómo fue utilizado, hace ya más de una década, un ordenador de este tipo por parte del Ministerio de Defensa de Guatemala para tener las listas de personas a "eliminar".

En un apartado distinto, el estudio analiza los sistemas de "privatización de cárceles", lo que significa el desarrollo de tecnologías que permiten sustituir la presencia de la policía -a veces mediante el uso de chips implantados- dentro de las cárceles. Otro, más adelante, expone el uso de "ciencia y tecnología para los mercados de interrogación y tortura tecnológica". En este capítulo se menciona explícitamente su "proliferación desde Estados Unidos y Europa" y se habla en especial del "uso y abuso de los daños producidos por electro shock y su proliferación". Recomienda el trabajo que se controle la venta de este tipo de material destinado a torturas.

LAS EMPRESAS DEL GRAN HERMANO

El estudio del Parlamento Europeo incluye la referencia de algunas de las numerosas empresas que, en la actualidad, se dedican a la investigación, desarrollo y fabricación de todos estos artilugios destinados al control de la población. Estas son algunas de ellas.

CELLMARK DIAGNOSTICS, de Gran Bretaña, sistemas de identificación por genes. Gran Bretaña es el primer país que ha puesto en marcha un banco de datos de DNA.

MASTIFF SECURITY SYSTEMS, Gran Bretaña, sistemas de identificación por el olor.

HAGEN CY-COM, Gran Bretaña, y Eyeidentify Inc., Estados Unidos, reconocimiento por el fondo de la retina.

AEA TECHNOLOGY, Gran Bretaña, identificación por sistemas mixtos.

ALLIANT TECH SYSTEMS, de Estados Unidos, trabaja en el desarrollo de armamento alternativo a las minas antipersonales.

LEUTCHER ASSOCIATES INC, de Massachussettes, de Estados Unidos, proporciona material para las ejecuciones. Su sistema más barato es el de la inyección letal, que cuesta unos 30.000 dólares, en tanto que la electrocución vale 35.000.

PK ELECTRONIC, de Alemania, versiones láser que pueden pinchar conversaciones que se desarrollan a través de una ventana cerrada, mediante la vibración del cristal.

E SYSTEMS, ELECTRONIC DATA SYSTEMS Y TEXAS INSTRUMENTS desarrollan y venden sistemas avanzados de vigilancia y control.

ROYAL ORDINANCE, de Gran Bretaña, HECKLER AND KOCH, de Alemania, VERNEY CARRON, de Francia, CROWN AIRCARTRIDGE, de Holanda, y las americanas MK BALLISTICS y MILSTOR CORP, fabrican balas no letales, destinadas a producir daños pero no a matar, con el fin de controlar movimientos de masas.

SIEMENS PLESSEY, vendió al Gobierno chino, en calidad de sistemas de control de tráfico, las cámaras que fueron utiliza-

das en la plaza de Tiananmen, en 1989, y para los trabajos posteriores de represión.



[Artículos sobre Derechos Humanos](#) | [España](#), [Echelon](#)