Ramonet, I. (2016) El imperio de la vigilancia. España. Clave Intelectual.

III
LAS REVELACIONES DE EDWARD SNOWDEN

«En el pasado, ningún gobierno había tenido el poder de mantener
a sus ciudadanos bajo una constante vigilancia.
Ahora, la Policía del Pensamiento vigila a todo el mundo, constantemente».

George Orwell, *1984*

La literatura (*1984*, de George Orwell) y el cine de ciencia ficción (*Minority Report*, de Steven Spielberg) nos habían alertado: con la instauración de las sociedades *securitarias* y los avances de las técnicas de la comunicación, acabaríamos todos bajo vigilancia. Pero pensábamos que, si esto llegaba a suceder, la violación de nuestra vida privada sería cometida por un régimen dictatorial de carácter neototalitario. Era un error. Las pasmosas revelaciones que el disidente estadounidense Edward Snowden hizo el 7 de junio de 2013 sobre la vigilancia orwelliana de nuestras comunicaciones, acusan directamente a los Estados Unidos, país generalmente considerado como la «patria de la libertad». Desde la ley *Patriot Act*, sabíamos a qué atenernos: los Estados no tardarían en persuadirnos para que digamos adiós a algunas de nuestras libertades. Además, el presidente Barack Obama acabó por confesarlo: «No podéis tener el 100% de seguridad, el 100% de respeto a la vida privada y cero inconve-

nientes. Es necesario que, como sociedad, elijamos[1]». Incluso, añadió, aunque ello implique «algunas modestas intromisiones en vuestra vida privada». ¿Modestas?

Volvamos a las declaraciones de Edward Snowden. Este exasesor técnico de la CIA, que entonces tenía 29 años y trabajaba para una empresa privada –*Booz Allen Hamilton*[2]– subcontratista de la NSA, reveló a Glenn Greenwald[3], periodista del diario británico *The Guardian*, y a Laura Poitras[4], realizadora de documentales cinematográficos, la existencia de programas ocultos, autorizados por el gobierno de los Estados Unidos, que permiten la vigilancia clandestina de las comunicaciones de millones de personas a través de todo el mundo.[5]

El programa PRISM

En el año 2006 se lanzó un primer programa secreto. Su finalidad: espiar todas las llamadas telefónicas realizadas, sobre todo a través de la compañía Verizon, tanto en el interior como hacia el exterior de los Estados Unidos.

Pero su principal revelación fue otro programa secreto, desarrollado por la NSA a partir de 2007, y cuyo nombre de

1. *L'Obs.*, 8 de junio de 2013.
2. En 2012, *Booz Allen Hamilton* facturó, a la Administración de los Estados Unidos, 1.300 millones de dólares por el servicio de «contribución a misiones de vigilancia».
3. Léase el testimonio de Glenn Greenwald, *Sin un lugar donde esconderse*, *op. cit.*
4. Autora del documental *Citizenfour*, que repasa las revelaciones de Edward Snowden sobre la vigilancia mundial generalizada, y que recibió el Oscar al mejor documental en 2015.
5. La Unión estadounidense para las libertades civiles ha reagrupado todos los documentos hechos públicos hasta ahora por Edward Snowden en la siguiente base de datos: https://www.aclu.org/nsa-documents-search

guerra es PRISM. Su objetivo: vigilar todas las comunicaciones procedentes del extranjero que pasan por los servidores de los Estados Unidos. En la práctica, el alcance de PRISM es mucho mayor. Permite a la NSA acceder totalmente a los servidores de nueve de las compañías de Internet más importantes, todas estadounidenses; o sea: AOL; Apple, Facebook[6], Google, Microsoft, Paltalk, Yahoo, Skype y YouTube (hay que destacar la ausencia de Twitter[7]).

Concretamente, la NSA puede obtener toda la información de cada una de estas empresas globales, lo que constituye el robo de datos personales más colosal de la historia, robo que afecta a miles de millones de personas que utilizan cada día los servicios de Facebook, Gmail, Skype o Yahoo en los cinco continentes. Los datos de cualquiera que, en los últimos diez años, haya utilizado los servicios de alguna de estas empresas, han sido, sin duda alguna, interceptados y almacenados por la NSA mediante la aplicación del programa PRISM. Conversaciones en audio y video, fotos, correos electrónicos, ficheros adjuntos, historial de las conexiones, chats en audio y video vía Skype, ficheros Google Drive, fototecas, claves de conexión... todo es espiado, filtrado, clasificado, archivado y transmitido a otras agencias de información de los Estados Unidos, a la CIA o al FBI, para verificaciones

6. El principal responsable de la seguridad antipiratería de Facebook, Max Kelly, encargado especialmente de proteger la información personal de los usuarios de Facebook contra los ataques exteriores, dejó la empresa en 2010, y fue contratado por... la NSA.
7. *Cf.* «L'absence de Twitter du programme PRISM, défense des libertés ou manque d'intérêt?», *Le Monde*, 11 de junio de 2013.

exhaustivas[8]. Según el *Washington Post*, los mil ojos de la NSA pueden «ver literalmente lo que usted teclea» en su ordenador[9].

Edward Snowden nos ha enseñado también –con pruebas– que la NSA tiene capacidad de activar a distancia los teléfonos móviles y los ordenadores (aunque estén apagados) y de transformarlos en dispositivos de escucha... «El teléfono que se lleva en el bolsillo –confirma Terry Hayes–, se puede encender a distancia sin que nos demos cuenta. De este modo se puede activar el micrófono que el móvil lleva integrado. En tal caso, quien se introduzca en el teléfono puede oír todo lo que se dice en una habitación[10].» Para protegerse contra esta intromisión, sólo hay que hacer una cosa: quitar la batería del teléfono (cuando se puede; en los iPhones, por ejemplo, ya no se puede) y meterlo en un frigorífico.

Controlar *todas* las comunicaciones

Otro documento difundido por Edward Snowden muestra que, en marzo de 2013, una unidad de la NSA, la *Global Access Operations*, recogió en apenas treinta días los metadatos de más de 124.000 millones de llamadas telefónicas y de más de 97.000 millones de correos electrónicos... Otros documentos, difundidos por *The Guardian* en junio de 2013, muestran también que, por término medio, la NSA roba mensualmente los metadatos de unos 13.500 millones de comunicaciones en la India y 2.300 millones en Brasil. Con la colaboración de los gobiernos y de los servicios de información locales, también captura los datos de alrededor de 500 millones de comunicaciones en Alemania, 70 millones en Francia, 60 millones en España, 47 millones en Italia, etc.[11]. Con un acopio tan colosal, PRISM sobrepasa todo lo que Orwell pudo imaginar. No es de extrañar que este programa secreto se haya convertido en la herramienta más eficaz a la hora de elaborar el informe diario sobre «riesgos en materia de seguridad», que la NSA remite cada mañana al presidente de los Estados Unidos.

> La NSA, explica Snowden, ha construido una formidable infraestructura que le permite interceptar prácticamente todo tipo de comunicaciones. De tal modo que esta agencia llega a almacenar la gran mayoría de las comunicaciones humanas, y puede hacer uso de ellas como quiera y cuando quiera[12].

Es algo tan enorme que le lleva a decir a Glenn Greenwald:

> El gobierno de los Estados Unidos ha creado un sistema cuyo objetivo es la eliminación total de la vida privada electrónica en el mundo. No es una exageración, es el objetivo explícito y literal de un Estado policiaco: proporcionar a la NSA todos los medios

8. La base legal que, en principio, autoriza esta vigilancia masiva es la *Foreign Intelligence Surveillence Act* (FISA), una ley de 1978 que describe los procedimientos de vigilancia física y electrónica, así como la recogida de informaciones en el extranjero, bien directamente, bien por medio del intercambio de información con otros gobiernos. En 2001, esta ley fue modificada por la *USA Patriot Act*, con el fin de incluir a los grupos terroristas. El 9 de julio de 2008, el Congreso votó una nueva modificación, la *FISA Amendments Act*, de 2008, para legalizar *a posteriori* las prácticas ilegales de escucha clandestina a ciudadanos estadounidenses en la era Bush. El 28 de diciembre de 2012, el Senado votó una prórroga de la ley hasta el 31 de diciembre de 2017. (Fuente: Wikipedia).
9. El único medio de evitar que el ordenador pueda ser vigilado a distancia es utilizar uno que *nunca* haya sido conectado a Internet. Los servicios de información solo podrían controlarlo accediendo físicamente a él e instalando un dispositivo de vigilancia («chivato») en su disco duro.
10. T. Hayes, *Yo soy Pilgrim*, *op. cit.*
11. G. Greenwald, *op. cit.*
12. E. Snowden, citado en *ibid.*

que le permitan recoger, almacenar, controlar y analizar todas las comunicaciones electrónicas entre todas las personas del mundo entero. La NSA está consagrada por completo a esta única misión: actuar de tal manera que ni una sola comunicación en el planeta escape a las garras de su sistema[13].

La Ley *USA Freedom Act*

En respuesta a una demanda interpuesta por la Unión estadounidense para las libertades civiles, la justicia de los Estados Unidos sentenció el 7 de mayo de 2015, a partir de estas revelaciones, que el programa de vigilancia de metadatos telefónicos –quién llama a quién, cuándo, dónde, cuánto tiempo– no tenía fundamento legal. El tribunal estimó que la sección 215 de la ley *Patriot Act* había sido utilizada erróneamente por la NSA y por el gobierno de los Estados Unidos. Esta sección 215 preveía que cualquier documento interno de una empresa podía ser requisado por las autoridades en nombre de la lucha contra el terrorismo. La Administración estadounidense sostenía que los metadatos telefónicos de los clientes de las empresas de telecomunicación no eran «*informaciones personales*». Sin embargo, según la Justicia, la NSA infringió realmente la ley al vigilar sin justificación legal a los ciudadanos estadounidenses[14]. Sin embargo, el Tribunal no ordenó el fin de la vigilancia. Por una sencilla razón: la sección 215 expiraba al final del mes de mayo de 2015... El 2 de junio de 2015, el Senado aprobó una nueva ley, la *USA Freedom Act*, que limita algunos de los

13. *Ibid.*
14. *Le Monde*, 7 de mayo de 2015.

excesos de la NSA en las tareas de vigilancia, aunque, en contrapartida, prolonga otras disposiciones de la *Patriot Act*. Esta nueva ley acaba sobre todo con la recogida masiva, automática e indiscriminada de metadatos, que continuarán almacenados en los operadores telefónicos; las autoridades podrán reclamarlos y acceder a ellos a medida que los vayan necesitando. Conservan la posibilidad de reclamarlos en tiempo real, pero tienen que justificar que existe un vínculo «razonable y detallado» con el terrorismo. La ley *USA Freedom Act* sólo afecta a la recogida de información en los Estados Unidos. No cambia nada sobre la vigilancia que la NSA practica clandestinamente en el extranjero[15].

La *National Security Agency*

En los Estados Unidos, el campo de la información permanece en el misterio. Por ejemplo, nadie conoce con exactitud el número de agencias que operan en él. Los mejores especialistas estiman que aproximadamente veintiséis de ellas son oficiales, y ocho más totalmente anónimas, de las que la opinión pública ignora incluso el nombre. El número de sus efectivos es también una información clasificada, aunque se puede razonablemente estimar en más de 150.000 el número de agentes que operan en su órbita. La más importante –y la más desconocida—de estas agencias es la NSA, que depende del Pentágono, es decir, del Ministerio de Defensa, y opera en todo el mundo. Es tan secreta que la mayoría de los estadounidenses desconocía su existencia hasta las revelaciones de Snowden, aunque, ya en

15. *Le Monde*, 4 de junio de 2015.

1998, una excelente película, *Enemigo público*[16], había denunciado ante la opinión pública el poder oculto de esta agencia.

El actor Gene Hackman interpretaba en ella el papel de un antiguo analista de transmisiones de la NSA, perfecto conocedor de la agencia y de sus fechorías:

> Tú telefoneas a tu mujer, explicaba en el film, y dices: «bomba», «presidente», «Alá»..., o un centenar de palabras similares, y el ordenador las analiza y las destaca... Esto ocurre desde hace décadas, porque, desde los años 1940, el Estado está compinchado con las empresas de telecomunicación y accede a todo: extractos bancarios, datos informáticos, correos electrónicos, llamadas telefónicas... Cuanto más enganchado estés a la tecnología, más fácil es ficharte. Antes, era necesario pincharte la línea, pero ahora los satélites la capturan directamente. La NSA tiene más de cien satélites-espía clasificados como secreto de defensa; y en su sede, en Fort Meade, dispone de una red informática subterránea de nueve hectáreas...

Por sí sola, la NSA emplea directamente a unos 30.000 agentes, y dispone además de aproximadamente 60.000 personas más, reclutadas por empresas privadas. De todos los presupuestos destinados a los servicios secretos estadounidenses, el más importante es el de la NSA. Ella, y no la CIA, es quien posee los principales sistemas de espionaje y control: una red mundial de satélites de vigilancia, millares de superordenadores, un número incalculable de agentes compiladores y descodificadores, e impresionantes bosques de gigantescas antenas satélites en las colinas del estado de Virginia Occidental. La

16. Tony Scoot, *Enemy of the State*, 1998.

NSA produce más de 50 toneladas de documentos clasificados cada día...

Una de las especialidades de la NSA es espiar a los espías, es decir, a los servicios de información de otras potencias, amigas y enemigas. Por ejemplo, durante la guerra de las Malvinas entre Argentina y el Reino Unido, en 1982, la NSA consiguió descifrar el código secreto de los servicios de información argentinos y transmitírselo a los británicos, proporcionándoles de esta forma una ventaja decisiva.

A principios de la década de 1990, la NSA no quiso ya limitarse a escuchar, vía satélite, el conjunto de los intercambios telefónicos y electrónicos en el mundo. Quiso ir más lejos, y pidió autorización para instalar un microchip pirata en cada ordenador o teléfono móvil fabricado en los Estados Unidos, para, de este modo, poder vigilar directa y clandestinamente las comunicaciones de estos aparatos electrónicos. Este proyecto totalitario, impulsado por el presidente Georges H. Bush padre (antiguo director de la CIA) fue, afortunadamente, parado por Bill Clinton en 1994.

Presidentes franceses bajo escucha

Otros documentos, revelados y difundidos por WikiLeaks el 24 de junio de 2015, y publicados en París por *Libération* y *Mediapart*, han mostrado que la NSA espió también a Francia. Incluso los tres últimos presidentes franceses –Jacques Chirac, Nicolas Sarkozy y François Hollande– fueron «escuchados» por agentes estadounidenses entre 2006 y 2012. Estos documentos, altamente reservados, nos han permitido tener una idea aproximada de la cantidad de información que la NSA puede interceptar sobre los principales responsables políticos franceses. Se trata

de informes analíticos procedentes de un trabajo de escucha, a diferencia de los documentos que difundió Snowden en 2013, que eran esencialmente fichas técnicas que describían las capacidades de la NSA.

Por ejemplo, uno de estos documentos lista los números de teléfono interceptados. Entre ellos, el del presidente francés en ese momento, Nicolas Sarkozy, y también los de algunos de sus colaboradores cercanos, como Jean-David Levitte (consejero diplomático) o Claude Guéant (en esa época, secretario general del Elíseo). En la lista está también el número de teléfono del portavoz de Asuntos Exteriores, el del secretario de Estado de Comercio Exterior (Pierre Lellouche) o el del de Asuntos Europeos (Jean-Pierre Jouyet). Y lo más preocupante: también aparece en ella el número de una sección telefónica del Eliseo encargada de las comunicaciones internas del ejecutivo.

Todos estos números figuran en una lista, establecida por la NSA, de «selectores», es decir, en la jerga de las agencias de información, de términos clave que les interesan especialmente (números de teléfono, direcciones electrónicas, etc.), lo que prueba que todas estas personalidades, entre ellas los tres presidentes franceses, fueron escuchadas directamente y sus conversaciones diseccionadas[17].

Otros documentos, difundidos por WikiLeaks en julio de 2015, muestran que los Estados Unidos espiaron también a otros aliados: en este caso, a los miembros del gobierno de Japón, incluido el primer ministro, Shinzo Abe, y su jefe de gabinete, Yoshihide Suga, así como a altos directivos del Banco Central nipón. En total, 35 «objetivos», entre los que se encontraban los patronos de importantes empresas industriales, fueron vigilados[18].

17. *Cf.* Adrien Gévaudan, «Affaire des écoutes de la NSA, pourquoi la France savait», *Revue Internationale et Stratégique*, 31 de octubre de 2013 (http://www.iris-france.org/43487-affaire-des-ecoutes-de-la-nsa-pourquoi-la-france-savait).

Otros jefes de Estado «amigos» –Dilma Rousseff, en Brasil, Enrique Peña Nieto, en México– fueron víctimas de las escuchas de la NSA. El semanario *Der Spiegel* reveló igualmente que el teléfono móvil de la canciller alemana Angela Merkel había sido escuchado por el *Special Collection Service* (SCS), una unidad de información muy especial, compuesta por miembros de la CIA y de la NSA. El *Spiegel* precisó que el SCS operaba desde el tejado de la Embajada de los Estados Unidos en Berlín. Se sabe que, en efecto, esta unidad disimula habitualmente sus aparatos de escucha en falsos edificios, camuflados a veces con trampantojos, y construidos con materiales especiales que dejan pasar fácilmente las ondas. Estos edificios se sitúan dentro del recinto de las embajadas o de los espacios consulares.

Embajadas, nidos de espías

Desde hace tiempo, hay instalados dispositivos de vigilancia en el último piso de la Embajada de los Estados Unidos en París, donde trabajan más de mil de personas, entre ellas miembros camuflados del SCS. No es casualidad que el edificio principal de la embajada esté situado en el corazón de todos los centros de poder francés. A menos de un kilómetro están el Eliseo, varios ministerios estatales (Interior, Justicia, Defensa, Asuntos Exteriores), la Asamblea Nacional...

Se sabe que las embajadas, sean del que país que sean, suelen ser nidos de espías, que se dedican a completar, de for-

18. *El País*, Madrid, 31 de julio de 2015.

ma ilegal, las informaciones recogidas abiertamente por los diplomáticos de carrera[19]. Tratándose de los Estados Unidos, esta particularidad alcanza proporciones desmesuradas. Desde hace mucho tiempo, este país se invistió a sí mismo de la función geopolítica de «potencia imperial»; así que sus embajadas en capitales extranjeras albergan innumerables servicios secretos.

Esto se puede observar con claridad en la película *Zero Dark Thirty*[20], que repasa de forma muy documentada la historia de la eliminación del jefe de Al Qaeda, Osama Bin Laden. Se descubre en ella que, sobre todo en países como Pakistán, Irak o Afganistán, las embajadas de los Estados Unidos ocultan en realidad impresionantes dispositivos de espionaje, gestionados por una multitud de agentes secretos y de expertos en seguimiento electrónico.

Otro testimonio de la inquietante realidad que esconde la mayoría de las embajadas de los Estados Unidos es el que nos entrega el fundador de WikiLeaks, Julian Assange:

> Todos los días laborables, 71.000 personas, en 191 países, que representan a diferentes agencias gubernamentales estadounidenses, se despiertan y se encaminan a su oficina. Tras haber franqueado las vallas de acero y las filas de guardias armados, acceden finalmente a alguno de los 276 edificios fortificados que componen las 169 embajadas y otras misiones diplomáticas del Departamento de Estado en el exterior. Allí se reúnen con los representantes y agentes de otros 27 ministerios y organismos del

19. En septiembre de 2010, WikiLeaks publicó unos 25.000 telegramas codificados, secretos, intercambiados entre el Departamento de Estado de los Estados Unidos y alrededor de 259 embajadas y consulados estadounidenses en todo el mundo. Estos telegramas pusieron de relieve el papel casi de procónsul que el embajador de los Estados Unidos ejerce en la mayoría de los países, en particular en España.
20. Kathryn Bigelow, *Zero Dark Thirty*, 2013.

> gobierno de los Estados Unidos, lo cual incluye a la CIA, a la NSA, al FBI y a las diferentes secciones de las fuerzas armadas encargadas de la información. [...] Entre ellos hay también agregados militares –espías al amparo del servicio exterior–, agentes de otras agencias gubernamentales de los Estados Unidos (incluso, en algunas embajadas, se pueden encontrar comandos encargados de operaciones especiales clandestinas). En el tejado de los edificios, potentes antenas de radio y satélite escrutan el cielo. Algunas están conectadas directamente con Washington para enviar (y recibir) mensajes del Departamento de Estado o de la CIA; otras sirven para repetir las comunicaciones de los barcos de guerra y los aviones militares que transitan por esos lugares; otras, en fin, han sido instaladas directamente por la NSA con el fin de vigilar masivamente los teléfonos móviles y las comunicaciones electrónicas de la población local[21].

Muy equipadas para las tareas de vigilancia, las embajadas estadounidenses se dedican seriamente a esta tarea. Como se ha visto, no dudan en espiar incluso a sus amigos. Y hay que constatar que, a pesar de sus débiles protestas, meramente formales, los aliados de los Estados Unidos parecen haberse resignado a vivir bajo la vigilancia permanente y clandestina de la NSA, un espionaje que constituye una seria amputación de su soberanía.

No se ha hecho nada al respecto. Algunos aliados, sobre todo los británicos y los alemanes, llegan incluso a colaborar con la agencia estadounidense que los espía. En mayo de 2015 se supo, por ejemplo, que, por cuenta de la NSA, los servicios

21. Julian Assange, http://readersupportednews.org/opinion2/277-75/32906-what-wikileaks-teaches-us-about-how-the-us-operates, 29 de agosto de 2015.

secretos alemanes (*Bundenaschrichtendienst*, BND) habían tenido bajo escucha en París, entre 2005 y 2015, a la presidencia de la República, al ministro de Asuntos Exteriores y a varias grandes empresas francesas, entre ellas Dassault y Airbus. Y que el dúo BND-NSA también había vigilado a los principales responsables políticos y económicos de otros países aliados: Bélgica, Países Bajos, Austria...

Según la prensa alemana, el BND estaría entregando mensualmente a la NSA hasta 1.300 millones de metadatos. Ya se ha visto que, aunque no revelen el contenido de las comunicaciones, estos metadatos permiten saber quién se ha comunicado con quién, durante cuánto tiempo y en qué lugar.

En España, según reveló la prensa, el Centro Nacional de Inteligencia (CNI) tambien facilitó el espionaje masivo de EE.UU. Los servicios de Inteligencia españoles conocían el trabajo de la Agencia Nacional de Seguridad estadounidense (NSA, en sus siglas en inglés) y le facilitaban sus tareas, según muestran varios documentos filtrados por Edward Snowden. Dicho de otro modo, el Centro Nacional de Inteligencia español habría permitido y ayudado a Washington a intervenir unos 60 millones de llamadas telefónicas en diciembre de 2012 y enero de 2013, violando de esta manera el derecho a la intimidad de los españoles.

El programa *Tempora*

Por su parte, los servicios de información británicos «escuchan» clandestinamente todas las comunicaciones que pasan por el Reino Unido. Espiaron incluso las comunicaciones de las delegaciones extranjeras que asistieron en Londres a la cumbre

del G20, en abril de 2008. Una vez más, sin hacer ninguna distinción entre enemigos y amigos[22].

Por otro lado, han puesto a punto su propio programa secreto de vigilancia electrónica, *Tempora*, que les permite acumular cantidades colosales de informaciones robadas. Sólo en 2012, el GCHQ habría vigilado unos 600 millones de «contactos telefónicos» ¡cada día! Con total ilegalidad, sus agentes habrían llegado a «conectarse» a más de 200 cables de fibra óptica... Cada cable transporta 10 gigabytes[23] por segundo. En teoría, los ordenadores del GCHQ pueden «tratar» unos 21 petabytes[24] al día, lo que significa «filtrar» el equivalente a los 40 millones de palabras de la *Enciclopedia Británica* ciento noventa y dos veces al día...

El objetivo de la NSA y de las agencias de información asociadas es controlar Internet y a sus más de 3.000 millones de usuarios. Parece imposible, pero están a punto de conseguirlo: «Empezamos a dominar Internet –ha declarado un espía inglés en *The Guardian*–, y nuestra capacidad actual es impresionante». Para mejorarla aún más, la agencia británica GCHQ lanzó en 2013 otros dos programas megalómanos: *Mastering The Internet* (MTI), sobre «cómo dominar Internet», e *Interception Modernisation Programme* (IMP), para una explotación definitivamente *orwelliana* de las telecomunicaciones globales.

---

22. En virtud de una ley aprobada por los conservadores británicos en 1994, que coloca el interés del Estado por encima de la cortesía diplomática, es legal espiar a los diplomáticos extranjeros en el Reino Unido.
23. En informática, el byte es la unidad de información. Un gigabyte (GB) es una unidad de almacenamiento de información, que equivale a 10^{10} bytes, es decir, a mil millones de bytes, el equivalente a una furgoneta totalmente cargada de hojas de papel escritas.
24. Un petabyte (PT) equivale a 10^{15} bytes.

Con el mismo fin, la NSA estableció hace tiempo acuerdos estratégicos con unas 80 empresas estadounidenses de electrónica, de telefonía y de servicios de ingeniería informática –entre ellas, AT&T, IBM, CSC, Microsoft, Oracle, Verizon, Intel, Motorola, Hewlett-Packard, EDS, Booz Allen Hamilton, Qalcomm, CenturyLink, Unisys, etc.–, que le prestan asistencia técnica en todas sus misiones. Son empresas gigantes que han puesto a punto las tecnologías operativas de vigilancia, y que velan por el buen funcionamiento de las infraestructuras y de los programas informáticos de las redes automáticas de espionaje.

La relación entre la NSA y estos socios privados adquiere una importancia estratégica para las autoridades de los Estados Unidos. Hasta tal punto que es supervisada por una de las unidades más secretas del sistema de información estadounidense: la *Special Source Operation* (SSO), que Edward Snowden no duda en calificar de «joya de la corona» de la NSA.

Gracias a los periodistas Duncan Campbell[25] y Nicky Hager[26] sabemos que, desde los años 1950, la NSA exige a las compañías telefónicas estadounidenses, especialmente a la *Western Union*, que, al final de cada jornada, envíen a un responsable de la agencia una copia de los metadatos del conjunto del tráfico de las telecomunicaciones que llegan a los Estados Unidos, o salen de ellos. Durante la investigación del caso Watergate, el director de la NSA fue interrogado y, en 1975, terminó por admitir: «La NSA intercepta sistemáticamente todas las comunicaciones internacionales, ya sean aéreas o por cable». Unos

25. Duncan Campbell es el autor del primer artículo sobre Echelon, publicado el 12 de agosto de 1988 por el semanario británico *New Statesman*.
26. Nicky Hager es autor del libro *Secret Power* (1996), en el que, por primera vez, desvela el funcionamiento de la red Echelon, y donde describe el papel que juega su país, Nueva Zelanda.

años después, un nuevo director de la agencia, John McConnell, confesará: «No hay ni un solo acontecimiento de la política extranjera que no interese al gobierno de los Estados Unidos, y en el que la NSA no esté directamente implicada[27]».

Los archivos difundidos por Snowden han mostrado que el coloso estadounidense de las telecomunicaciones, AT&T, también había autorizado secretamente a la NSA para que accediera a miles de millones de correos electrónicos intercambiados en el territorio estadounidense, entre ellos los de la sede de Naciones Unidas, en Nueva York, cuyo proveedor de acceso a Internet es AT&T. Paralelamente, se ha sabido también que AT&T suministraba a la agencia de Fort Meade más de mil millones de lecturas de móviles *al día*[28].

El complejo *securitario-digital*

Es completamente inédita esta alianza entre el poder político, el aparato de información, algunos grandes medios de comunicación dominantes, y los titanes tecnológicos que controlan las telecomunicaciones, la electrónica, la informática, Internet, las industrias de fibra óptica por cable, los satélites, los programas informáticos, los servidores, etc. Una complicidad de este calibre, entre la primera potencia militar del mundo y las empresas privadas globales que dominan las nuevas tecnologías de Internet, instituye de hecho un auténtico complejo *securitario-digital*, que sucede al complejo militar-industrial, denunciado por el presidente Eisenhower en 1960, un complejo que amenaza

27. http://echelononline.free.fr/pages/chrono.html
28. *Le Monde*, 18 de agosto de 2015.

con tomar el control del Estado democrático. Sus características más inquietantes son precisamente la banalización de la vigilancia masiva y la tentación del control social integral.

Este reforzamiento sin precedentes de la prepotencia del Estado y esta amplia privatización del espionaje, están creando, en democracia, una nueva entidad política –el Estado de vigilancia– frente a cuyo poder el ciudadano se siente cada vez más desarmado y desamparado.

IV
UNA GUERRA DE CUARTA GENERACIÓN

¡Tened espías en todas partes!
Sun Tzu, *El arte de la guerra*

Todas estas leyes del tipo *Patriot Act*, que pisotean el derecho al anonimato y a la vida privada de millones de personas, y que han sido calificadas de «liberticidas» por numerosas organizaciones de defensa de los derechos humanos[1], son consecuencia también de una nueva doctrina militar: la de la «guerra permanente y sin límites». Para las autoridades estadounidenses en primer lugar, pero también, y poco a poco, para los gobiernos de otros países, Francia y España entre ellos, el peso de la amenaza de terroristas o de movimientos insurgentes no estatales, camuflados en el seno de la población urbana, obliga a alcanzar un nivel más sofisticado de información mediante tecnologías punta. «En nuestra lucha contra el terrorismo –ha declarado,

1. *Cf.*, por ejemplo, la campaña francesa «Stop à la surveillance de masse», lanzada por Amnesty International (http:www.amnesty.fr/Nos-campagnes/Liberte-expression/Actions/Stop-la-surveillance-de-masse-14551). La página web de la campaña española de Amnistía internacional es la siguiente: https://www.es.amnesty.org/dejendeseguirme/ [N. del T.].

por ejemplo, el presidente Obama– necesitamos disponer de todos los instrumentos eficaces[2].»

Según esta doctrina, la guerra asimétrica contemporánea, sobre todo contra el fenómeno yihadista (tanto el de Al Qaeda como, más recientemente, el del Estado Islámico, o Daesh), y muy especialmente contra sus «células durmientes» y, sobre todo, contra la figura del «lobo solitario», refuerza drásticamente el recurso permanente a técnicas militarizadas de rastreo y de selección de objetivos en los espacios de la vida cotidiana.

Efectivamente, como explica el geógrafo británico Stephen Graham[3], esta «guerra de cuarta generación» se desarrolla cada vez más en espacios urbanos: estaciones, estadios, teatros, supermercados, oficinas, apartamentos, galerías comerciales, pasillos del metro, suburbios industriales, aeropuertos... «De este modo, la ciudad se encuentra en el centro de las preocupaciones de los responsables militares y de seguridad, a la vez como espacio donde los poderes occidentales son vulnerables, y como campo de las batallas que hay que librar contra los enemigos de Occidente[4].»

Insectos voladores robotizados

En consecuencia, la respuesta de las autoridades ha consistido en multiplicar las estrategias de vigilancia y de control recurriendo a nuevas herramientas de espionaje, en gran parte

2. *Rue89* (http://rue89.nouvelobs.com) 31 de mayo de 2015.
3. Stephen Graham, *Villes sous contrôle. La militarisation de l'espace urbain*, trad., fr. de R. Toulouse, París, La Découverte, 2012. Edición original: *Cities Under Siege: The New Military Urbanism*, Verso, Londres, 2011.
4. Éric Verdeil, «Stephen Graham, *Villes sous contrôle. La militarisation de l'espace urbain*», Lectures, 25 de agosto de 2012 (http://lectures.revues.org/9021).

accionadas a distancia: perfil de los individuos, vigilancia de los lugares, comprobación de los comportamientos, etc.; empleando todas las tecnologías de seguimiento disponibles: video, escáner biométrico, satélites, drones[5], cámaras infrarrojas; y todas las técnicas de captación de datos: huellas digitales o de la palma de la mano, lectura del iris, cotejo del ADN, reconocimiento de la voz, del rostro y del peso, medición de la temperatura por láser, análisis comparado del olor y de la forma de andar, insectos voladores robotizados (o «dronizados») que penetran en el interior de los edificios para observar al enemigo y su armamento[6]...

Todo esto supone una auténtica invasión de la vida privada de los ciudadanos por una serie de detectores, generalmente invisibles y conectados unos con otros, con capacidad para escudriñar todos los actos y gestos. Chris Anderson, antiguo redactor jefe de la revista *Wired*, y fundador de 3Drobotics, una empresa de fabricación de robots, cree que esta tendencia continuará y se acelerará. Prevé que, en un futuro próximo, con la proliferación de drones, «habrá millones de cámaras volando por encima de nuestras cabezas[7].» Estos drones se basarán en el «*pattern of life*»: si una persona presenta unas «pautas de vida» semejantes «visualmente» a las de una persona considerada «peligrosa», será señalada y eliminada. Nunca se conocerá su nombre; la identidad importa menos que la eliminación física de alguien que *se parece* a un «terrorista peligroso[8].» Nos diri-

5. Véase A. Gévaudan, «Drones de combat», *Ragemag*, 7 de enero de 2014 (http://ragemag.fr/drone-combat-asimov-herbert-present-59198).
6. *Cf.* Anna Minton, «Attention, un robot volant vous espionne», *Courrier international*, 1 de abril de 2010.
7. *El País*, Madrid, 31 de agosto de 2015.
8. A. Gévaudan, «Drones: tu le sens bien, mon gros MALE?», *Ragemag*, 27 de mayo de 2013 (http://ragemag.fr/drones-t-le-sens-bien-mon-gros-male-29770).

gimos así hacia un mundo semejante al que imaginó, en 1987, el novelista británico Arthur C. Clarke en su relato de ciencia ficción *2061: Odysea tres*[9]. La acción se desarrolla en la «era de la transparencia», en un mundo donde la paz y el orden están garantizados por una permanente vigilancia universal mediante enjambres de satélites.

¡Nuestro televisor nos escucha!

Sin esperar a 2061, en nuestra vida cotidiana dejamos constantemente rastros que entregan nuestra identidad, dejan ver nuestras relaciones, reconstruyen nuestros desplazamientos, identifican nuestras ideas, desvelan nuestros gustos, nuestras elecciones y nuestras pasiones, incluso las más secretas. A lo largo del planeta múltiples redes de control masivo no paran de vigilarnos. En todas partes, alguien nos observa a través de nuevas cerraduras digitales. El desarrollo de la Internet de las cosas (*Internet of Things*) y la proliferación de aparatos conectados[10], multiplican la cantidad de chivatos de todo tipo que nos cercan. En Estados Unidos, por ejemplo, la empresa de electrónica Vizio, instalada en Irvine (California), principal fabricante de televisores inteligentes conectados a Internet, ha revelado recientemente que sus televisores espiaban a los usuarios por medio de tecnologías incorporadas en el aparato.

9. Este libro es el tercero de una tetralogía de novelas cuyos otros títulos en español son: *2001: Una odisea espacial, 2010: Odisea dos, 2061: Odisea tres* y *3001: Odisea final*
10. Se habla de objetos conectados para referirse a aquellos cuya misión primordial no es, simplemente, la de ser periféricos informáticos o *interfaces* de acceso a la Web, sino la de aportar, provistos de una conexión a Internet, un valor suplementario en términos de funcionalidad, información, interacción con el entorno, o de uso (Fuente: *Dictionnaire du Web*).

Los televisores graban todo lo que los espectadores consumen en materia de programas audiovisuales, tanto los programas de las cadenas por cable, como los DVD, los paquetes de acceso a Internet o las consolas de videojuegos... Por lo tanto, Vizio puede saberlo todo sobre las selecciones que sus clientes prefieren en materia de ocio audiovisual. Y, consecuentemente, puede vender esta información a empresas publicitarias que, gracias al análisis de los datos acopiados, conocerán con precisión los gustos de los usuarios y estarán en mejor situación para tenerlos en el punto de mira[11].

Esta no es, en sí misma, una estrategia diferente de la que, por ejemplo, Facebook y Google utilizan habitualmente para conocer a los internautas y ofrecerles publicidad adaptada a sus supuestos gustos. Recordemos que, en la novela de Orwell *1984*, los televisores –obligatorios en cada domicilio–, «ven» a través de la pantalla lo que hace la gente («¡Ahora podemos veros!»). Y la pregunta que plantea hoy la existencia de aparatos tipo Vizio es saber si estamos dispuestos a aceptar que nuestro televisor nos espíe.

Si lo juzgamos por la denuncia interpuesta, en agosto de 2015, por el diputado californiano Mike Gatto contra la empresa surcoreana Samsung, parece que no. La empresa era acusada de equipar sus nuevos televisores también con un micro oculto, capaz de grabar las conversaciones de los telespectadores, sin que éstos lo supieran, y transmitirlas a terceros[12]... Mike Gatto, que preside la Comisión de protección del consumidor y de la vida privada en el Congreso de California, presentó incluso una

11. *El País*, Madrid, 2015.
12. A partir de entonces, Samsung anunció que cambiaría de política, y aseguró que, en adelante, el sistema de grabación instalado en sus televisores sólo se activaría cuando el usuario apretara el botón de grabación.

proposición de ley para prohibir que los televisores pudieran espiar a la gente.

Por el contrario, Jim Dempsey, director del centro «Derecho y Tecnologías», de la Universidad de California, en Berkeley, piensa que los televisores-chivatos van a proliferar: «La tecnología permitirá analizar los comportamientos de la gente. Y esto no sólo interesará a los anunciantes. También podría permitir la realización de evaluaciones psicológicas o culturales, que, por ejemplo, interesarán también a las compañías de seguros[13]». Sobre todo teniendo en cuenta que las empresas de recursos humanos y de trabajo temporal ya utilizan sistemas de análisis de voz para establecer un diagnóstico psicológico inmediato de las personas que les llaman por teléfono en busca de empleo...

Nunca más solos

Repartidos un poco por todas partes, los detectores de nuestros actos y gestos abundan alrededor de nosotros, incluso, como acabamos de ver, en nuestro televisor: sensores que registran la velocidad de nuestros desplazamientos o nuestros itinerarios; tecnologías de reconocimiento facial que memorizan la impronta de nuestro rostro y crean, sin que lo sepamos, bases de datos biométricos de cada uno de nosotros ... Por no hablar de los nuevos chips de identificación por radiofrecuencia (RFID)[14], que descubren automáticamente nuestro perfil de consumidor, como hacen ya las «tarjetas de fidelidad» que generosamente ofrece la mayoría de los grandes supermercados (Carrefour, Ca-

13. *El País*, Madrid, agosto de 2015.
14. Que ya forman parte de muchos de los productos habituales de consumo, así como de los documentos de identidad.

sino, Alcampo, Erozki) y las grandes marcas (FNAC, el Corte Inglés, Galeries Lafayette, Printemps).

Ya no estamos solos frente a la pantalla de nuestro ordenador. ¿Quién ignora a estas alturas que son examinados y filtrados los mensajes electrónicos, las consultas en la Red, los intercambios en las redes sociales? Cada clic, cada uso del teléfono, cada utilización de la tarjeta de crédito y cada navegación en Internet suministra excelentes informaciones sobre cada uno de nosotros, que se apresura a analizar un imperio en la sombra al servicio de corporaciones comerciales, de empresas publicitarias, de entidades financieras, de partidos políticos o de autoridades gubernamentales.

El necesario equilibrio entre libertad y seguridad corre, por tanto, el peligro de romperse. En la película de Michael Radford, *1984*, basada en la novela de George Orwell, el presidente supremo, llamado *Big Brother*, define así su doctrina: «La guerra no tiene por objetivo ser ganada, su objetivo es continuar»; y: «La guerra la hacen los dirigentes contra sus propios ciudadanos, y tiene por objeto mantener intacta la estructura misma de la sociedad[15].» Dos principios que, extrañamente, hoy están a la orden del día[16] en nuestras sociedades contemporáneas. Con el pretexto de tratar de proteger al conjunto de la sociedad, las autoridades ven en cada ciudadano a un potencial delincuente. La guerra permanente contra el terrorismo les proporciona una coartada moral impecable, y favorece la acumulación de un impresionante arsenal de leyes y dispositivos para proceder al control social integral.

15. Michael Radford, *1984*, 1984.
16. *Cf. Infra*, nuestra entrevista con Noam Chomsky, pp. 137 y ss.

Y más teniendo en cuenta que la crisis económica aviva el descontento social que, aquí o allí, podría adoptar la forma de motines ciudadanos, levantamientos campesinos o revueltas en los suburbios. Más sofisticadas que las porras y las mangueras de las fuerzas del orden, las nuevas armas de vigilancia permiten identificar mejor a los líderes y ponerlos anticipadamente fuera de juego.

Sociedades de control

«Habrá menos intimidad, menos respeto a la vida privada, pero más seguridad», nos dicen las autoridades. En nombre de ese imperativo se instala así, a hurtadillas, un régimen *securitario* al que podemos calificar de «sociedad de control[17].» En la actualidad, el principio del «panóptico» se aplica a toda la sociedad. En su libro *Surveiller et punir*, el filósofo Michel Foucault explica cómo el «panopticon[18]» («el ojo que todo lo ve») es un dispositivo arquitectónico que crea una «sensación de omnisciencia invisible», y que permite a los guardianes ver sin ser vistos dentro del recinto de una prisión. Los detenidos, expuestos permanentemente a la mirada oculta de los «vigilantes», viven con el temor de ser pillados en falta. Lo cual les lleva a autodisciplinarse... De donde podemos deducir que el principio organizador de una sociedad disciplinaria es el siguiente: bajo la presión de una vigilancia ininterrumpida, la gente acaba por modificar su comportamiento. Como afirma Glenn Greenwald:

17. *Cf.* A. Mattelart, *La Globalisation de la surveillance*, París, La Découverte, 2007; edición en español: *Un mundo vigilado*, Paidós, 2009.
18. Imaginado en 1791 por el filósofo utilitarista inglés Jeremy Bentham.

> Las experiencias históricas demuestran que la simple existencia de un sistema de vigilancia a gran escala, sea cual sea la manera en que se utilice, es suficiente por sí misma para reprimir a los disidentes. Una sociedad consciente de estar permanentemente vigilada se vuelve enseguida dócil y timorata[19].

Hoy día, el sistema panóptico se ha reforzado con una particularidad nueva en relación a las anteriores sociedades de control que confinaban a las personas consideradas antisociales, marginales, rebeldes o enemigas en lugares de privación de libertad cerrados: prisiones, penales, correccionales, hospitales psiquiátricos, asilos, campos de concentración... Sin embargo, nuestras contemporáneas sociedades de control dejan en libertad aparente a los sospechosos (es decir, a *todos* los ciudadanos), aunque los mantienen bajo vigilancia electrónica permanente. La contención digital ha sucedido a la contención física.

Google lo sabe todo de ti

A veces, esta vigilancia constante también se lleva a cabo con ayuda de chivatos tecnológicos que la gente adquiere *libremente*: ordenadores, teléfonos móviles, tabletas, abonos de transporte, tarjetas bancarias inteligentes, tarjetas comerciales de fidelidad, localizadores GPS, etc. Por ejemplo, el portal Yahoo!, que consultan regular y voluntariamente unos 800 millones de personas, captura una media de 2.500 rutinas al mes de cada uno de sus usuarios. En cuanto a Google, cuyo número de usuarios sobrepasa los mil millones, dispone de un impre-

19. G. Greenwald, *Nulle part où se cacher*, *op. cit.*

sionante número de sensores para espiar el comportamiento de cada usuario[20]: el motor *Google Search*, por ejemplo, le permite saber dónde se encuentra el internauta, lo que busca y en qué momento. El navegador *Google Chrome*, un megachivato, envía directamente a Alphabet (la empresa matriz de Google) todo lo que hace el usuario en materia de navegación. *Google Analytics* elabora estadísticas muy precisas de las consultas de los internautas en la Red. *Google Plus* recoge información complementaria y la mezcla. *Gmail* analiza la correspondencia intercambiada, lo cual revela mucho sobre el emisor y sus contactos. El servicio *DNS* (*Domain Name System*, o Sistema de nombres de dominio) de Google analiza los sitios visitados. *YouTube*, el servicio de videos más consultado del mundo, que pertenece también a Google y, por tanto, a Alphabet, registra todo lo que hacemos en él. *Google Maps* identifica el lugar en que nos encontramos, adónde vamos, cuándo y por qué itinerario... *AdWords* sabe lo que queremos vender o promocionar. Y desde el momento en que encendemos un *smartphone con Android*, Google sabe inmediatamente dónde estamos y qué estamos haciendo. Nadie nos obliga a recurrir a Google, pero cuando lo hacemos, Google sabe todo de nosotros. Y, según Julian Assange[21], inmediatamente informa de ello a las autoridades estadounidenses...

En otras ocasiones, los que espían y rastrean nuestros movimientos son sistemas disimulados o camuflados, semejantes a los radares de carretera, los drones o las cámaras de vigilancia (llamadas también de «videoprotección»). Este tipo de cámaras ha proliferado tanto que, por ejemplo, en el Reino Unido, don-

20. Leer «Google et le comportement de l'utilisateur», *AxeNet* (http://blog-axe-net-fr/google-analyse-comportement-internaute).
21. *Cf. Infra* nuestra entrevista, pp. 111 y ss.

de hay más de cuatro millones de ellas (una por cada quince habitantes), un peatón puede ser filmado en Londres hasta 300 veces cada día. Y las cámaras de última generación, como la Gigapan, de altísima definición –más de mil millones de píxeles–, permiten obtener, con una sola fotografía y mediante un vertiginoso zoom dentro de la propia imagen, la *ficha biométrica* del rostro de cada una de las miles de personas presentes en un estadio, una manifestación o un mitin político[22].

A pesar de que hay estudios serios que han demostrado la débil eficacia de la videovigilancia[23] en materia de seguridad, esta técnica sigue siendo refrendada por los grandes medios de comunicación. Incluso una parte de la opinión pública ha terminado por aceptar la restricción de sus propias libertades: el 63% de los franceses se declara dispuesto a una «limitación de las libertades individuales en Internet en razón de la lucha contra el terrorismo[24]». Lo cual demuestra que el márgen de progreso en materia de sumisión es todavía considerable.

Una nueva concepción de la identidad parece emerger. Muchas personas no tienen ningún inconveniente en responder a encuestas en la Red sobre su intimidad y sus gustos en materia de lecturas, moda, cine, gastronomía, sexualidad, viajes, etc. Les gusta que Internet los conozca mejor para poder recibir propuestas personalizadas, adaptadas a su perfil...

22. Véase, por ejemplo, la foto de la ceremonia de la primera investidura del presidente Obama, el 20 de enero de 2009, en Washington (http://gigapan.org/viewGigapanFullscreen.php?auth=033ef14483ee899496648c2b4b06233c).
23. «Assessing the impact of CCTV», el más exhaustivo de los informes dedicados al tema, publicado en febrero de 2005 por el Ministerio del Interior británico (*Home Office*), asesta un golpe muy duro a la videovigilancia. Según este estudio, la debilidad del dispositivo se debe a tres elementos: la ejecución técnica, la desmesura de los objetivos asignados a esta tecnología, y el factor humano». (Noé Le Blanc, «Sous l'oeil myope des caméras», *Le Monde diplomatique*, septiembre de 2008).
24. *Le Canard enchaîné*, 15 de abril de 2015.

Sociedades exhibicionistas

Hay que reconocer que muchas personas se burlan de la protección de la vida privada, y reclaman, por el contrario, el derecho a mostrar y exhibir su intimidad. Esto puede sorprender, pero si se reflexiona sobre ello, un manojo de señales y síntomas anunciaba, desde hace algún tiempo, la ineluctable llegada de este tipo de comportamientos, que mezcla inextricablemente *voyeurismo* y exhibicionismo, vigilancia y sumisión.

Su matriz lejana se encuentra, quizás, en una célebre película de Alfred Hitchcock, *Rear Window* (*La ventana indiscreta*, 1954), en la que un reportero gráfico (James Stewart), convaleciente en su casa, con una pierna escayolada, observa por ociosidad el comportamiento de sus vecinos de enfrente. En un diálogo con François Truffaut, Hitchcock explicaba: «Sí, el personaje era un *voyeur*, pero ¿no somos todos *voyeurs*?». Truffaut lo admitía: «Todos somos *voyeurs*, aunque sólo sea cuando vemos una película intimista. Por otro lado, James Stewart se encuentra, en su ventana, en la misma situación de un espectador que ve una película». Entonces, Hitchcock observaba: «Apuesto a que si alguien, al otro lado del patio, ve a una mujer que se desnuda antes de acostarse, o simplemente a un hombre que está ordenando su habitación, nueve de cada diez personas no podrán dejar de mirar. Podrían mirar para otro lado y decirse: 'esto no va conmigo', podrían cerrar las contraventanas... Pero ¡no lo harán!, se quedarán mirando[25]».

A esta pulsión *escópica* de mirar, de vigilar, de espiar, le corresponde, como contrapunto, su contrario: el gusto impúdico

25. François Truffaut, *Le Cinéma selon Hitchcock*, París, Robert Laffont, 1966; edición en español: *El cine según Hitchcock*, Alianza, 1996.

por exhibirse, que, con el apogeo de Internet, ha conocido una especie de explosión a través de las *webcam*, sobre todo a partir de 1996. Aún recordamos, por ejemplo, a los cinco estudiantes, chicos y chicas, de Oberlin, en Ohio (Estados Unidos) que, al principio de la moda de las *webcam*, se exhibían en línea (www.hereandnow.net) todos los días, a todas las horas del día, en cualquier lugar de las dos plantas de su vivienda. Vivían vigilados por unas cuarenta cámaras, colocadas voluntariamente por todas partes. Desde entonces, miles de personas, solteros, parejas, familias, invitan sin pudor a los internautas de todo el mundo a compartir su intimidad y a observar cómo viven sin prácticamente ninguna censura[26].

Otro signo del poco apego que algunas personas tienen a la protección de su vida privada: los diarios íntimos, que se han multiplicado en la Web. En otro tiempo secretos y personales, los diarios íntimos y las autobiografías circulan ahora libremente por la Red. Cada vez más personas entregan, sin censura, a la masa de internautas sus pensamientos más íntimos, sus sentimientos más ocultos, tratando de compartir su intimidad.

Incluso se vio por primera vez a un chino, Lu Yuqing, escribir directamente en la Red su *Diario de muerte*, que se convirtió en un auténtico fenómeno global de literatura electrónica. Al saber que tenía los días contados, este joven agente inmobiliario de Shanghái decidió compartir con sus contemporáneos su lucha contra el cáncer de estómago que lo consumiría hasta el último suspiro: «Corto la cinta. Os quiero[27]».

26. Véase Denis Duclos, «La vie privée traquée par les technologies», *Le Monde diplomatique*, agosto de 1999; y Paul Virilio, «Le règne de la délation optique», *Le Monde diplomatique*, agosto de 2000.
27. *Le Monde*, 14 de noviembre de 2000.

Por otra parte, desde principios de los años 2000, las emisiones conocidas como «*TrashTV*», o «telebasura», que mostraban a personas que, sin ningún pudor, narraban sus problemas más íntimos o sus pasiones más ocultas, se multiplicaron en los programas de la televisión generalista estadounidense. La más conocida de ellas era el *Jerry Springer Show*, donde los invitados al plató hacían confidencias escandalosas sobre su vida privada ante un público que deliraba. Visto por más de ocho millones de telespectadores, este programa recibía cada semana miles de llamadas de estadounidenses dispuestos a contarlo todo sobre su vida privada a cambio de quince minutos de fama.

Con el título «Es mi elección», la cadena pública *France 3* adoptó, en Francia, una idea parecida –«con gente de verdad que habla de su vida de verdad»–, que obtuvo un triunfo de audiencia (siete millones de adeptos) y provocó vivas polémicas[28].

Incluso los propios asesinos no quieren ya ocultar nada, y ahora se apresuran a confesarlo todo sobre su vida criminal. La cadena estadounidense por cable *Court TV*, especializada en la difusión de confesiones de asesinos, fue la primera del mundo en presentar, con un realismo sórdido, «las confesiones de Steven Smith, que cuenta la violación y el asesinato de un médico en un hospital de Nueva York, en 1989, así como las de Daniel Rakowitz, que, también en 1989, mató a una amiga y después la descuartizó e hirvió los pedazos de su cuerpo; y las de David García, un prostituto que describe el asesinato, en 1995, de un cliente inmovilizado en una silla de ruedas[29]»...

28. *Libération*, 25 de noviembre de 2000; *Le Monde*, 30 de noviembre de 2000.
29. *Le Monde*, 25 de agosto de 2000.

Soplones voluntarios

En la actualidad, millones de personas exponen públicamente en las redes sociales detalles personales de su biografía o de sus actividades cotidianas. Con total despreocupación. No parece inquietarles el que ellas mismas se coloquen un brazalete electrónico virtual que permite a los nuevos *Big Brothers* seguirles la pista. Mientras, en alguna parte, unas máquinas acumulan una cantidad infinita de datos sobre ellas. Sin duda, esta nueva concepción de la identidad es la que empuja también a miles de personas a alistarse en diferentes servicios de policía como confidentes voluntarios. Por ejemplo, el Departamento de Justicia de los Estados Unidos, bajo la presidencia de George W. Bush, lanzó en 2002 la Operación TIPS (*Terrorism Information and Prevention System*) –tip significa soplo, chivatazo–, dirigida a transformar en confidentes a millones de profesionales cuya especialidad los lleva a entrar en las casas de la gente: repartidores, fontaneros, albañiles, cerrajeros, electricistas, antenistas, carteros, técnicos del gas, jardineros, empleados de mudanzas, empleados domésticos, etc. Cientos de ellos se comprometieron a contactar con la policía si advertían cualquier «señal sospechosa».

Uno de los objetivos de la guerra de «cuarta generación», es pasar así de una sociedad informada a una sociedad de informantes. Este es exactamente el objetivo de la *Texas Border Sheriff's Coalition*, que hizo instalar varios centenares de cámaras de vigilancia[30] en emplazamientos aislados y estratégicos a lo largo de la frontera entre Texas y México. Estas cámaras están conectadas a Internet (www.blueservo.net) y cualquier persona

30. https://www.youtube.com/eatch?v=5wsXKjeM3LE

en cualquier parte del mundo puede espiar sin riesgo las zonas desérticas de Texas o las orillas de Río Grande sentada cómodamente delante de su ordenador. Si en su pantalla ve pasar a un emigrante clandestino, lo puede denunciar enviando simplemente un correo a las autoridades. Unos treinta millones de individuos con espíritu de soplones han aceptado ya, en muchos países, llevar a cabo esta función de «informante voluntario» de la policía tejana de fronteras...

En el Reino Unido, la empresa *Internet Eyes* lanzó una iniciativa parecida en 2009, presentada como una especie de juego abierto a todos los internautas. También en este caso, el objetivo es vigilar comercios y calles rastreando las posibles infracciones. Para adherirse y participar en el sistema, los voluntarios tienen que pagar una pequeña cuota mensual. Una vez comprobada su identidad, tienen acceso a las imágenes de cuatro cámaras de vigilancia, que aparecen en su ordenador.

Sentados en su sillón, los miembros observan en directo, a través del objetivo de las cámaras. Si detectan un robo, una agresión, un comportamiento sospechoso, hacen clic en un botón de alerta. Entonces la imagen se congela y tienen la posibilidad de ampliarla para verificar. Acto seguido, el encargado del local recibe un mensaje con la imagen seleccionada. Si considera útil este aviso, el internauta-delator obtiene tres puntos. Si considera que el aviso fue justificado, aunque finalmente no haya habido infracción, el internauta recibe un punto. Por el contrario, si el comerciante considera que la alerta es injustificada, el «vigilante» no recibe ningún punto y hasta puede perder alguno. *Internet Eyes* promete al internauta-espía que haya detectado más fraudes o robos una recompensa a final de mes que puede alcanzar las 1.000 libras esterlinas...

Entrevistado por el diario londinense *The Telegraph*, el creador de este sitio web, Tony Morgan, se justifica: «Hay más de cuatro millones de cámaras de vigilancia, pero sólo se mira una de cada mil. De esta manera, se observan las cámaras veinticuatro horas al día. Es la mejor arma de prevención de delitos que jamás se haya inventado». Por el contrario, los que se oponen a la videovigilancia consideran que esta página web es un peligro –«atenta contra la vida privada y es una herramienta de espionaje»– porque deja a la vista de todos las caras y los comportamientos de los clientes de los comercios[31]. Algunas asociaciones han denunciado el hecho de que el sitio permita que los vecinos se espíen, y que pueda ser utilizado por verdaderos delincuentes para analizar los hábitos de los locales con el fin de robarles de manera más efectiva.

Con la multiplicación de los éxodos migratorios y el ascenso de la xenofobia en Europa, se puede suponer que algunas autoridades europeas se sientan tentadas a instalar un sistema semejante de cámaras conectadas a Internet, sabiendo que probablemente podrán contar con una legión de soplones civiles voluntarios.

Una de las perversiones de nuestras sociedades de control es esta: hacer que los ciudadanos sean vigilantes y vigilados al mismo tiempo. Cada uno debe espiar al otro, al tiempo que él mismo es espiado. De este modo, en un marco democrático donde los individuos están convencidos de que viven en la mayor de las libertades, se avanza hacia el objetivo soñado por las sociedades más totalitarias.

---

31. http://www.lepetitjournal.com/londres/societe/70129-surveillance-internet-eyes-is-watching-you-

Internet en 2030

La CIA se interesa también por estos fenómenos desde un punto de vista geopolítico. El *National Intelligence Council* (NIC), la oficina de análisis y de anticipación geopolítica y económica de la CIA, publica cada cuatro años, al comienzo de un nuevo mandato presidencial en los Estados Unidos, un informe que automáticamente se convierte en la referencia principal de todas las cancillerías del mundo. Aunque se trata, evidentemente, de una visión muy parcial (la de Washington), elaborada por una agencia –la CIA– cuya misión principal es defender los intereses de los Estados Unidos, este informe estratégico del NIC tiene un interés indiscutible porque es el resultado de una puesta en común –revisada por todas las agencias de información estadounidenses– de los estudios elaborados por expertos independientes de muchos países y de varias universidades internacionales.

El documento confidencial que el presidente Barack Obama encontró encima de su escritorio de la Casa Blanca el 21 de enero de 2013, día en el que iniciaba su segundo mandato, fue publicado con el título Global *Trend 2030. Alternative Worlds* («Tendencias mundiales 2030: nuevos mundos posibles»)[32]. ¿Qué dice sobre la sociedad de vigilancia?

Según los investigadores de la CIA, en el Nuevo Sistema Internacional, algunas de las mayores colectividades del mundo ya no serán países sino «comunidades agrupadas y vinculadas a través de Internet y de las redes sociales», Por ejemplo, *Facebooklandia*: más de mil millones de usuarios; o *Twitterlandia*: más de 800 millones. Su influencia en el juego de tronos de la

32. http://www.dni.gov/index.php/about/organization/national-intelligence-council-global-trends. En francés se publicó con el título *Le Monde en 2030 vu par la CIA*, París, éditions des Équateurs, 2013.

política mundial podría ser decisiva. Por lo tanto, en los próximos años las estructuras de poder podrían dispersarse en función del acceso universal a la Red y a las nuevas herramientas digitales.

A este respecto, el informe de la CIA anuncia la aparición de tensiones entre los ciudadanos y ciertos gobiernos, tensiones que algunos sociólogos califican de «pospolíticas» o «posdemocráticas»... Por una parte, la generalización del acceso a Internet y la universalización del uso de las nuevas tecnologías permitirán a los ciudadanos ampliar el campo de sus libertades y desafiar a sus representantes políticos (como fue el caso de las «primaveras árabes» o de la irrupción de los «indignados» en España). Pero, al mismo tiempo, estos mismos instrumentos electrónicos proporcionarán a los gobiernos, según los autores del informe, «una capacidad sin precedentes para vigilar a sus ciudadanos».

> La tecnología –señalan los analistas de *Global Trends 2030*– seguirá siendo el gran elemento de diferenciación de los Estados, pero los futuros emperadores de Internet, semejantes a los de Google o Facebook, poseerán montañas enteras de datos, y manipularán en tiempo real mucha más información que los Estados.

En consecuencia, la CIA recomienda al presidente de los Estados Unidos que se prepare para enfrentarse a las grandes empresas privadas que controlan Internet, activando el *Special Collection Service*[33], un servicio de información ultrasecreto, especializado en la captación clandestina de informaciones de origen electromagnético, que depende conjuntamente de la

33. http://en.wikipedia.org/wiki/Central_Security_Service.

NSA y del SCB (*Service Cryptologic Elements*) de las fuerzas armadas.

La CIA cree que si un grupo de empresas privadas llegara a controlar la masa de datos que circula en Internet, podría *condicionar el comportamiento* de una gran parte de la población mundial, incluso de las instituciones gubernamentales. La CIA teme también que, en un futuro próximo, el terrorismo yihadista sea reemplazado por un ciberterrorismo aún más peligroso y destructor[34].

34. Para tener una idea de la destrucción y el caos que podría provocar un ciberataque masivo contra los sistemas informáticos estadounidenses, véase la película *Die Hard 4: Retour en Enfer* (2007), realizada por Len Wiseman con un guión de Mark Bomback y David Marconi (autor del guión de *Enemigo de Estado*) basado en el artículo de John Carlin, «A Farewell to Arms», *Wired*, 5 de mayo de 1997. (Esta película se estrenó en España con el título *La jungla 4.0*, y en América Latina, con el de *Duro de matar 4.0*)

CONCLUSIÓN

Hoy todos los estadounidenses están bajo escucha.
Edward Snowden

A nuestro alrededor merodea permanentemente un *Big Brother* que quiere saberlo todo de cada uno de nosotros, y clasificarnos en función de los «riesgos potenciales» que podríamos presentar. Esta vigilancia masiva ha sido siempre la gran tentación de los poderes autoritarios. En este sentido, algunos regímenes del pasado permanecen definitivamente asociados a prácticas secretas de intromisión en la vida de las personas. Pensamos sobre todo en el III Reich hitleriano y en el Estado estalinista. En su novela *1984*, George Orwell se burló especialmente de este último. Más próxima a nosotros, la película *La vida de los otros*[1] ha estigmatizado el sistema de vigilancia generalizada en la antigua República Democrática Alemana (RDA), implantado por el Ministerio para la Seguridad del Estado, más conocido como Stasi.

Estos regímenes eran dictaduras. Pero, en nuestros días, son democracias las que han levantado sofisticadas redes de vigilancia clandestina, a veces en contradicción con sus

1. Florian Henckel von Donnersmarck, *Das Leben der Anderen*, 2006.